RAND CORPORATION

Research Report

DEVIN TIERNEY, BRADLEY WILSON, HANSELL PEREZ, AUGUSTINE BRAVO, MEGAN McKERNAN, THOMAS GOUGHNOUR

Quantifying Vulnerability Lifespans for U.S. Marine Corps Joint Cyber Weapons

RAND researchers were asked to assist the Joint Cyber Weapons (JCW) program office in refining key acquisition artifacts that are required during the planning phase of the software acquisition pathway within the Department of Defense's Adaptive Acquisition Framework (Department of Defense Instruction 5000.87, 2020).[1] One of those artifacts is a Lifecycle Cost Estimate, which uses information about the lifespan of cyber vulnerabilities that can

KEY FINDINGS

- Because of the uncertainty surrounding vulnerability life spans and cyber weapon complexity, the estimated costs for the JCW program range from approximately $125 million to $375 million over five years to maintain at least five working weapons.
- Collection of open-source data about cyber vulnerabilities presents challenges because of a lack of both precise common vulnerabilities and exposures (CVE) temporal data and uniformity across sources.
- Across the nine product categories that were used to categorize vulnerabilities in this report, minor software update frequencies display a range from an average of every 20 days for mobile phones to 178 days for industrial control systems, which indicates the short timelines under which JCW must operate.
- Enterprise information technology (IT) infrastructure and non-enterprise IT infrastructure vulnerabilities had longer historic average life spans than other categories of software at averages of 1,115 and 1,078 days, respectively, which suggests that there is less cost to develop exploits for software in these categories.
- An expansion of the developed CVE dataset might reveal additional life span trends. However, the lack of a viable automated data collection method limits the scope of CVE-related analysis.

Abbreviations

CVE	common vulnerabilities and exposures
CVE DS 1	Common Vulnerabilities and Exposures Dataset 1
CVE DS 2	Common Vulnerabilities and Exposures Dataset 2
CC	cyber capability
DS	dataset
FY	fiscal year
IT	information technology
JCW	Joint Cyber Weapons
MARCORSYSCOM	U.S. Marine Corps Systems Command
OS	operating system

be leveraged for operational purposes. This analysis builds on previous companion research that developed a cost estimating framework for cyber weapon investment that combined data on schedule, risk, and operational capability. The framework captured demand requirements for cyber capabilities (CCs),[2] uncertainties surrounding vulnerability decay rates and weapon development costs, variable adversary defense capabilities, and time phasing of acquisitions into service. Recommendations from that research and the analysis in this report focus on quantifying uncertainties around the lifespans of vulnerabilities and further understanding the associated tradespace of cyber weapon acquisition cost, schedule, and risk to assist the JCW program's support of the U.S. Marine Corps' cyber needs (Wilson et al., 2023).

Objective and Approach

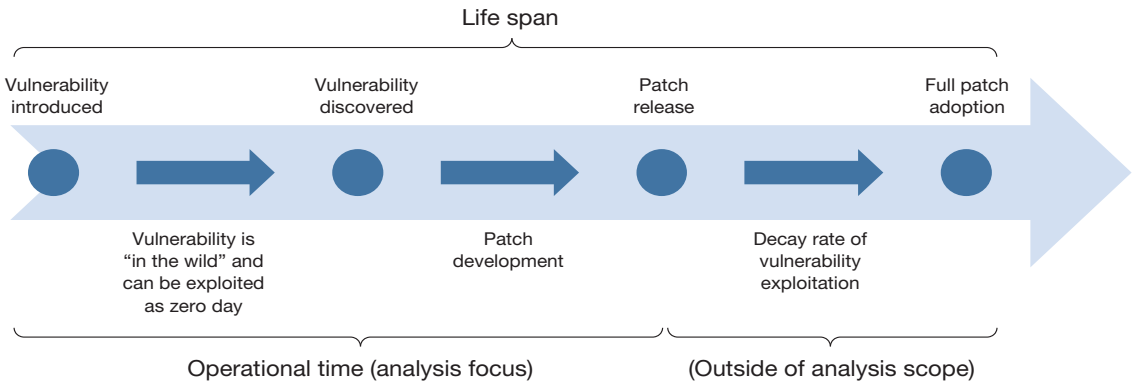
In Wilson et al. (2023), an exploratory model was presented that evaluated investment scenarios under varying assumptions of cyber weapon cost, development time, and operational time for U.S. Marine Corps Systems Command's (MARCORSYSCOM's) JCW acquisition program. Open-source data related to the lifespan of zero day exploits were collected to inform model parameters, although both the number and fidelity of sources presented challenges.[3]

As part of the prior analysis, seven areas of potential enhancement to the model were identified. This report builds on the prior work in two main areas: increasing the granularity of cyber weapon types, and further developing and parameterizing the adversary defense level decay functions for exploits.[4] To accomplish this, we gathered additional open-source datasets that document characteristics of thousands of known CVEs. One challenge presented by these data is that the length of time between when a vulnerability was initially introduced and when it was detected is often unknown. Additionally, the type, target environment, severity, and other characteristics of vulnerabilities and related exploits vary widely. In this report, we attempt to gather a subset of exploited vulnerabilities that contain similar attributes to cyber weapons that might be developed. We gathered a record of relevant exploited vulnerabilities, applied a common high-level categorization to attempt to group similar data, and developed a set of data for common software major and minor release dates, all with the intent of developing a better understanding of vulnerability lifespan.

Figure 1 is a general representation of the events across the lifespan of a vulnerability. The lifespan of a vulnerability is from the introduction of the vulnerability to when a system running the vulnerable software is patched. Typically, vulnerability introduction dates and full patch adoption dates are not known. We computed the operational time for identified vulnerabilities using the delta between the most recent major software update prior to the discovery of the vulnerability and the patch release date.[5] We use the most recent major software update before vulnerability discovery as a proxy for the vulnerability introduction date. To further explore the assumption that we used to estimate operational time, we gathered the update cadences of major and minor software updates across various products and vendors to serve as separate comparison datasets. These software update datasets are used as a proxy for operational time. We assume that a vulnerability is introduced in one update and the subsequent software update patches that vulnerability. In this way, the dates of the two updates can be used for the vulnerability introduction and patch release date, respectively.

The details of the data sources used and manipulation of the gathered data are discussed in the following section.

FIGURE 1
Key Events in the Life Span of a Vulnerability



SOURCE: Adapted from Wilson et al., 2023.
NOTE: The most recent major software update prior to the "vulnerability discovered" date was used as a proxy for the "vulnerability introduced" date.

Data Sources and Preparation

The MITRE Corporation's CVE program and the National Institute of Standards and Technology National Vulnerabilities Database both catalog cybersecurity vulnerabilities (Common Vulnerabilities and Exposures Program, undated; National Institute of Standards and Technology, undated). Additionally, there are private-sector efforts to catalog zero-day vulnerabilities. For this effort we used three of those datasets: Google's Project Zero (Google, 2023), Cybersecurity Help s.r.o.'s Zero-Day Tracking Project (Zero-Day Tracking Project, undated), and Trend Micro's Zero Day Initiative (Zero Day Initiative, undated). Because each data source is a living document, the cutoff for data used was August 2022.

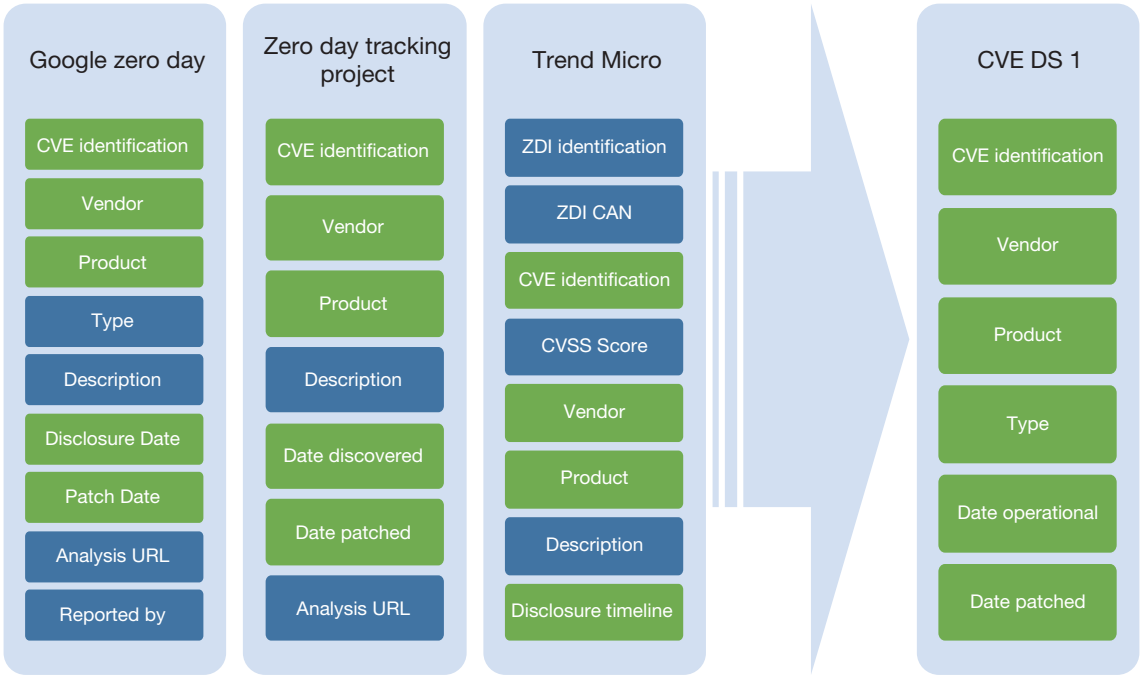
Google's Project Zero documents zero-day vulnerabilities that were subsequently exploited; it was foundational to our analysis. These data provided such information as CVE identification, vendor and product affected, vulnerability type and description, vulnerability disclosure date and patch date, links to more-descriptive analysis, and who reported the vulnerability. We combined the Project Zero data with data from Cybersecurity Help's Zero-Day Tracking Project. From Cybersecurity Help, we extracted CVE identification numbers, vendor, product, description, date discovered, date patched, and advisory URL. We refer to this combined dataset as CVE Dataset 1 (CVE DS 1). Only those vulnerabilities with an identified patch date were included in the final CVE DS 1 dataset. We then included a subset of vulnerabilities identified in the Trend Micro data to increase the number of observations for certain types of vulnerabilities with a low number of data points observed. Figure 2 summarizes the fields gathered from each data source.

We manually investigated and assigned estimated operational time. Table 1 summarizes the sources used to create CVE DS 1 and the number of CVEs gathered from each, totaling 233 CVE data points.

Because of time challenges in manually estimating operational time in data collected for CVE DS 1, we created a second dataset by automating the process of collecting CVE information and patch development times using the Trend Micro data source. We randomly sampled 10 percent of all vulnerabilities listed from years 2014 to 2022 in the Trend Micro Zero Day Initiative database and collected 746 unique vulnerabilities. These vulnerabilities contained a wide variety of unique vendors and products that were not necessarily closely tied to the types found in the other two data sources. The CVE data from Trend Micro contains disclosure dates and patch dates but lacks the introduction date necessary to estimate operational time. We were able to align 320 of the 746 data points with the nine product categories used in this analysis and created a second dataset, CVE Dataset 2 (CVE DS 2), that specifically focused on the patch development time section

FIGURE 2

Data Source Fields for CVE DS 1



NOTE: To be included in the combined CVE dataset CVE DS 1, a vulnerability must have both a listed patch date and an identified date for its introduction, per Figure 1. The green boxes show the items from each database that were incorporated into the CVE DS 1 dataset for analysis. CAN = Common Access Number; CVSS = Common Vulnerability Scoring System; ZDI = Zero Day Initiative.

of total operational time. The sections that follow describe the data sources and combined dataset in more detail.

Limitations and Assumptions

There are certain caveats for CVE DS 1 that should be noted. Dates attained for analysis might slightly deviate from actual dates. This deviation is because of a standard industry practice of developing and implementing a patch as a response to a CVE then reporting the problem to the consumers. Doing so eliminates some risk for exploitation of the CVE from other parties. Another issue is that many companies do not keep a detailed history of every patch and update performed. As a result, we manually identified other user-created archives that might not be as accurate as desired when searching for previous software updates. Because multiple resources were used to manually gather data, it should be noted that the process is not straightforward. CVE DS 1 shown in the following section might contain noise because

TABLE 1

Data Sources for Combined Operational Time for CVE DS 1

Source	Vulnerabilities Included in Our Analysis
Google Project Zero	171
Cybersecurity Help s.r.o. Zero-Day Tracking Project	44
Trend Micro Zero Day Initiative	18
Total	233

NOTE: Data points gathered are from 2014 to 2022.

of incomplete information from a variety of definitive sources. Continuing to develop the assembled data to be more comprehensive could improve the dataset, but doing so would require a significant amount of manual research time.

Some vendors and types of CVEs appear more frequently because of data fidelity or popularity of products. Dates and version histories are generally recorded more consistently by companies whose products are widely integrated into everyday use and have large numbers of global users, such as Google, Linux, and Apple. Major companies, such as Microsoft and Apple, often provide publicly available detailed version history records. Some products allow users to back trace to previous versions required for specific product features, which creates a strong archive of version histories.

Product Category Data

The compiled CVEs in CVE DS 1 and CVE DS 2 were categorized into nine high-level product categories to explore potential trends in lifespan lengths and patch development times related to the target of a vulnerability. We created categories to establish a common classification method across the varied data sources. The eight product categories used by Zerodium, a zero-day acquisition and research platform, provided a starting point that was tailored to align with product categories of interest for this analysis.[6] The following nine product categories are used to classify the data:

- **desktop operating systems:** standard operating systems (OSs) used commonly across desktop platforms, such as Microsoft Windows, Apple iOS, and Linux
- **desktop software:** general use software that can be installed on standard operating systems, including such common internet browsers as Microsoft Office, Google Chrome, and Microsoft Edge
- **enterprise cybersecurity:** programs related to cybersecurity used commercially or by private consumers, such as firewall software
- **enterprise IT infrastructure:** programs used commercially for day-to-day operations and general use to complete business, such as the Microsoft Exchange server
- **industrial control systems:** hyperspecific programs created for operation of particular equipment (i.e., supervisory control and data acquisition or SCADA systems)
- **internet services and websites:** services that provide a niche role or plug-in software, such as Tor and virtual private network services.
- **mobile and smartphones:** OSs for phones and software applications that can be installed to mobile platforms, such as Apple iOS, Google Android, and mobile apps
- **non-enterprise IT infrastructure:** private consumer products used in home internet connections and networks, such as routers, modems, and internet of things
- **web development infrastructure software:** tools used in IT development environments to construct applications and other software, such as Silverlight or WebKit

Vulnerabilities gathered during data collection were assigned product categories for analysis. All 233 items in CVE DS 1 were assigned a product category; 320 of the 746 vulnerabilities from the Trend Micro dataset could be associated with one of the nine categories.

Software Update Cadence Data

One factor that is potentially correlated to the times described previously, lifetime and patch development time, is the software update frequency of a product (e.g., new minor and major version releases). To examine this factor, we collected timelines for selected products in the datasets. For a given product, we searched for documentation that listed the dates on which updates were issued. Software updates were categorized as either major or minor. We define *major* as a change in version type and *minor* as additions to said version of the software.

With the available relevant information, a dataset was created that contained fields identifying the vendor, product, type of update, and date of update.[7] Each unique product in the assembled software update cadence dataset was classified into one of the nine product categories.

The process of collecting these data presented similar challenges to the CVE DS 1 (e.g., incomplete information, varied data fidelity across sources). During this process, we found that not all vendors provide detailed documentation for their products or a centralized repository in which the desired information could be found. For example, although Google has an established website where one can find all updates issued for Chrome—including version numbers, dates issued, and update descriptions—other products do not have an easily accessible information source. The information sourced to assemble a record of software update cadence varied from official product documentation to security bulletins on updates to specific product versions. It is worth repeating that the development of the timelines is a manual process of searching the web for the necessary information, which, depending on vendor and product, does not guarantee a useful update history.

In some cases, third-party or user-created timelines for updates, versions, and histories were the only reliable source. Another data-collection challenge was general updates that were listed without specific version numbers or specific dates. The update cadence dataset gathered is limited to vendors and products for which the update version and date information were identifiable. A list of the vendors and products included in the software update cadence dataset can be found in the appendix.

Common Vulnerabilities and Exposures Analysis

In this section, we explore operational times from CVE DS 1, the patch development time of additional vulnerabilities gathered from Trend Micro in CVE DS 2, and the software update cadence dataset. We walk through descriptive figures of the types of vulnerabilities gathered in the data by vendor, product, and assigned product category. Summaries of vulnerabilities by product category, ranges of estimated operational times, patch development times, and time between updates are also displayed. We then used statistics from these data to construct inputs for the exploratory model to examine the impact of varying assumptions related to significant uncertainties around vulnerability lifespans.

CVE DS 1 Analysis

Figure 3 shows the number of vulnerabilities by vendor for CVE DS 1. Only the top ten most-common vendors are shown out of a total of 38 vendors. The full list can be found in the appendix. Figure 4 breaks out the CVEs by vendor product, again showing only the top ten most-common vendors. All 56 products are listed in Table A.2.

Each CVE in CVE DS 1 contains a disclosure date, patch date, and an estimated operational time. Well-known vendors, such as Microsoft, account for most CVEs in the data, which might reflect the large product catalogs and user bases and high levels of vulnerability tracking and reporting in those organizations.

CVE DS 2 Analysis

Figure 5 shows the top ten vendors and the count of their CVEs in CVE DS 2 during the effort to automate data collection using the Trend Micro data, with the full list in Table A.3.

CVEs in this dataset contain disclosure and patch dates but do not have an estimated operational lifespan. Similar to the combined CVE dataset, familiar vendors such as Adobe and Apple appear frequently in the data.

Like Figure 4, which shows data from CVE DS 1, Figure 6 shows the top ten (of 79) products in CVE DS 2; many CVEs represent widely used products, including OSs and internet browsers. The full list can be found in Table A.3.

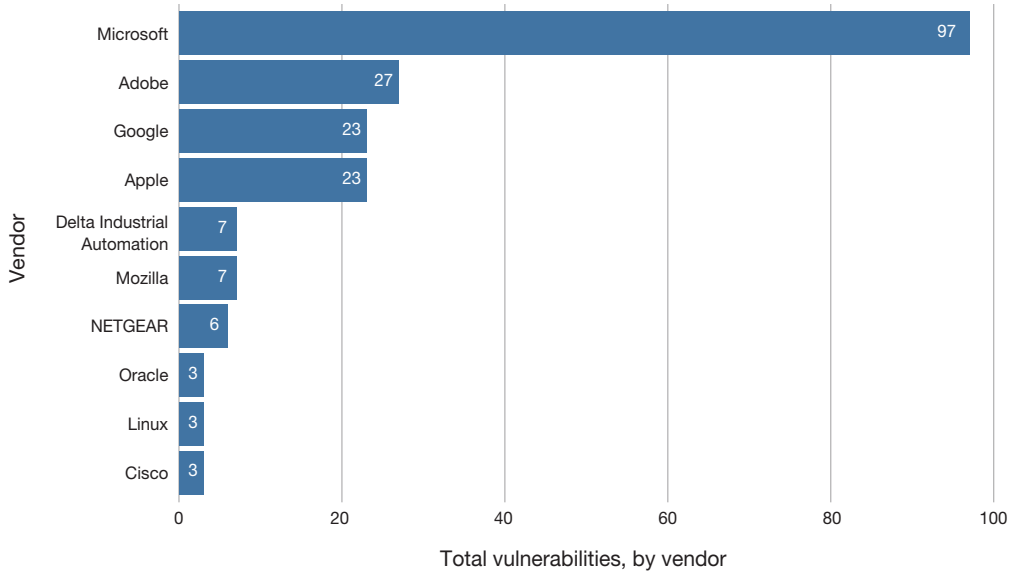
As in the CVE DS 1, this pattern might be tied to their popularity rather than to specific product attributes.

Product Category Analysis

Products in CVE DS 1 and CVE DS 2 were categorized into the nine product categories. The categorizations represent our best assessment. However, there is likely room for discussion on appropriate categorizations. We found that CVEs in the product catego-

FIGURE 3

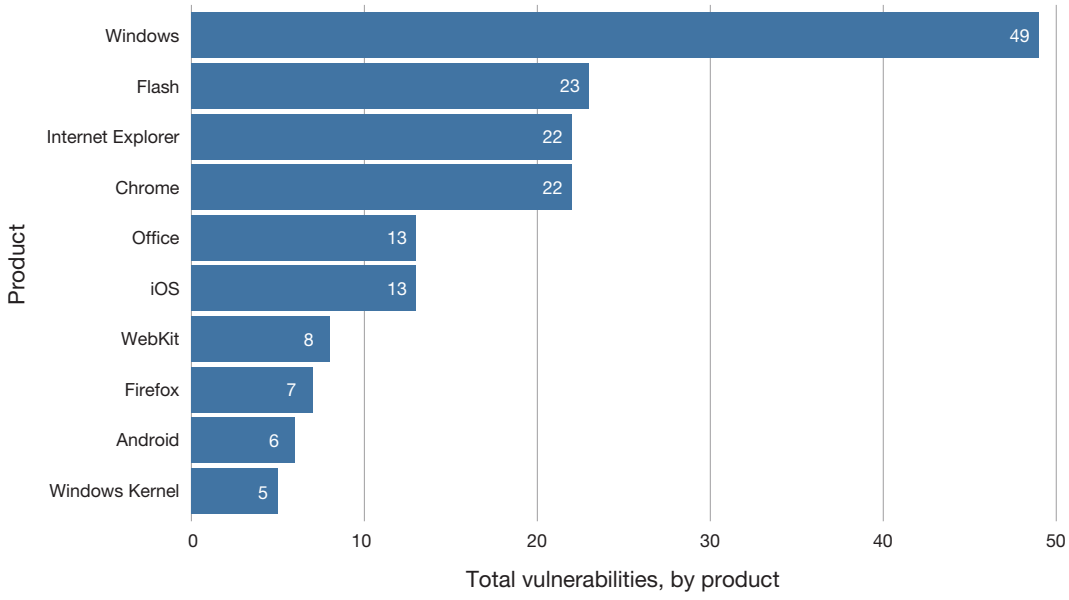
Vulnerability Count, by Vendor, for CVE DS 1



SOURCE: Authors' analysis of data from Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated. The data displayed constitute 199 of 233 vulnerabilities in CVE DS 1 from ten of 38 identified vendors.

FIGURE 4

Vulnerability Count, by Product, for CVE DS 1



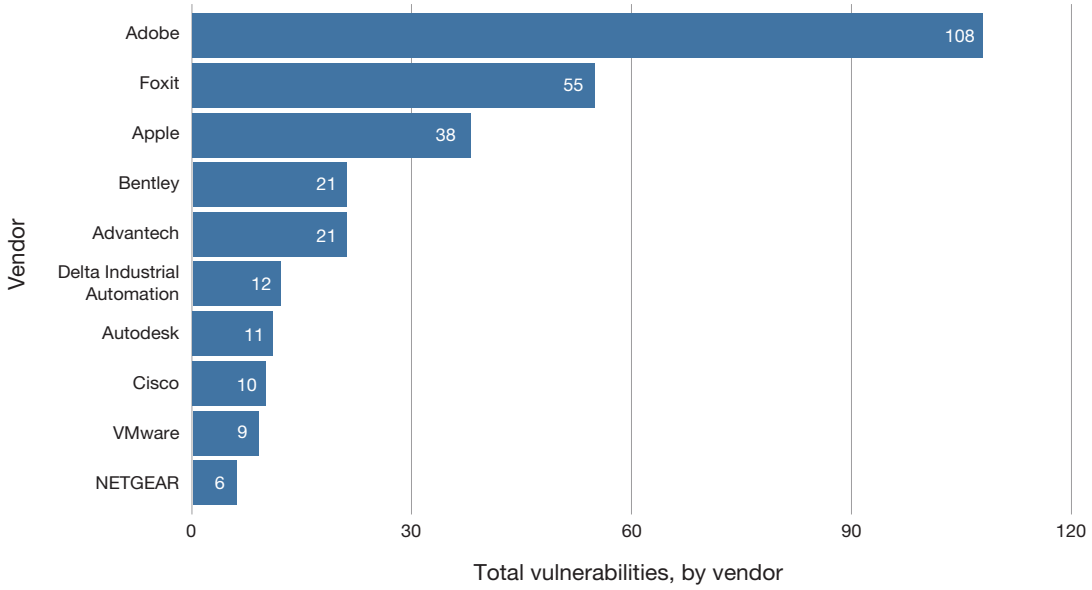
SOURCE: Authors' analysis of data from Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated. The data displayed constitute 168 of 233 vulnerabilities in CVE DS 1 from ten of 56 products identified.

ries of desktop software and desktop OSs account for the majority of the analysis data; categories of non-enterprise IT infrastructure and internet services or websites are less represented.

CVEs that were specific to the patch data collected from Trend Micro in CVE DS 2 were also grouped into the nine product categories shown. Product categories were manually assigned to CVEs

FIGURE 5

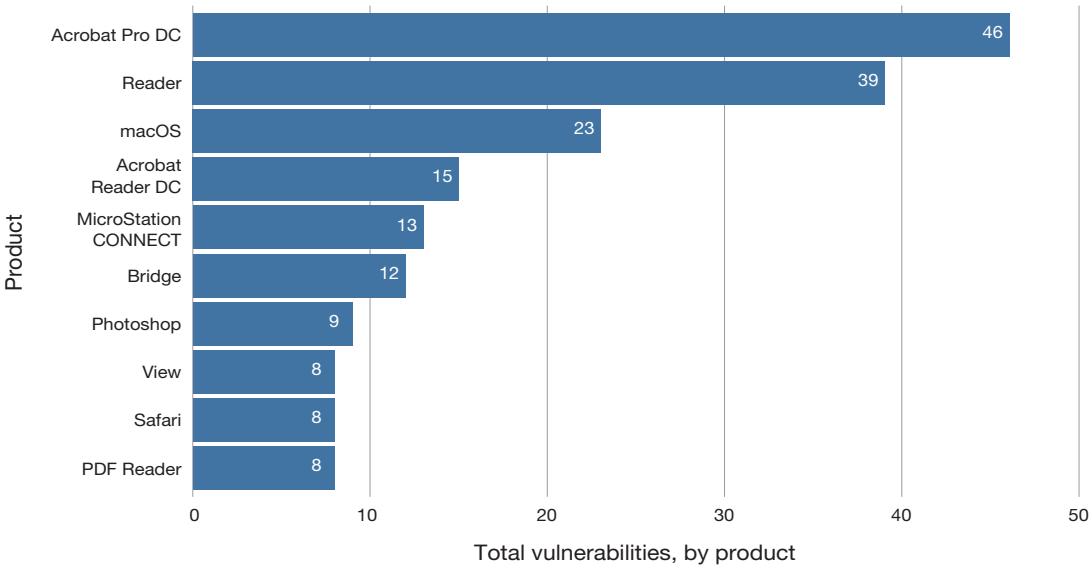
Vulnerability Count, by Vendor, for CVE DS 2



SOURCE: Authors' analysis of data from Trend Micro Zero Day Initiative, undated. The data displayed constitute 291 of 320 vulnerabilities in CVE DS 2 from ten of 31 vendors identified.

FIGURE 6

Vulnerability Count, by Product, for CVE DS 2



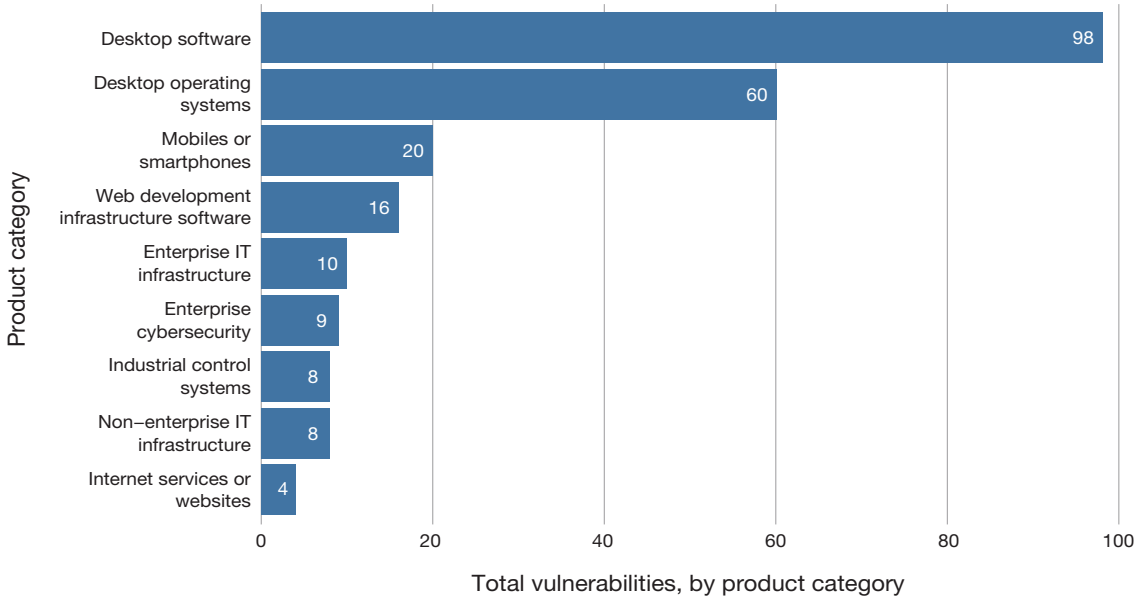
SOURCE: Authors' analysis of data from Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated. The data displayed constitute 168 of 233 vulnerabilities in CVE DS 1 from ten of 56 products identified.

to examine potential trends across groupings of CVEs that contain similarities. Similar to the CVE DS 1 data shown in Figure 7, Figure 8 shows that CVEs in the product categories of desktop software occur most frequently, .

Enterprise IT infrastructure and industrial control systems are more represented in CVE DS 2 than

FIGURE 7

Vulnerability Count, by Product Category, for CVE DS 1



SOURCE: Authors' analysis of data from Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated. The data displayed constitute all vulnerabilities in CVE DS 1.

they are in CVE DS 1. Additional vulnerabilities were gathered from Trend Micro Zero Day Initiative that were not manually assigned into product categories because of time constraints. Classifying additional vulnerabilities could add further richness to the dataset.

Figure 9 shows a box plot of estimated operational lifespan by product category in CVE DS 1 using the delta between the most recent major release date before vulnerability disclosure and the vulnerability patch release date. There are some noticeable outliers that represent years of estimated operational time and several product categories that fall into a similar range of estimated operational times.

Figure 10 displays a truncated version of Figure 9. Some selected data are not displayed to more easily visualize the comparative ranges of operational times across product categories with shorter estimated lifespans.

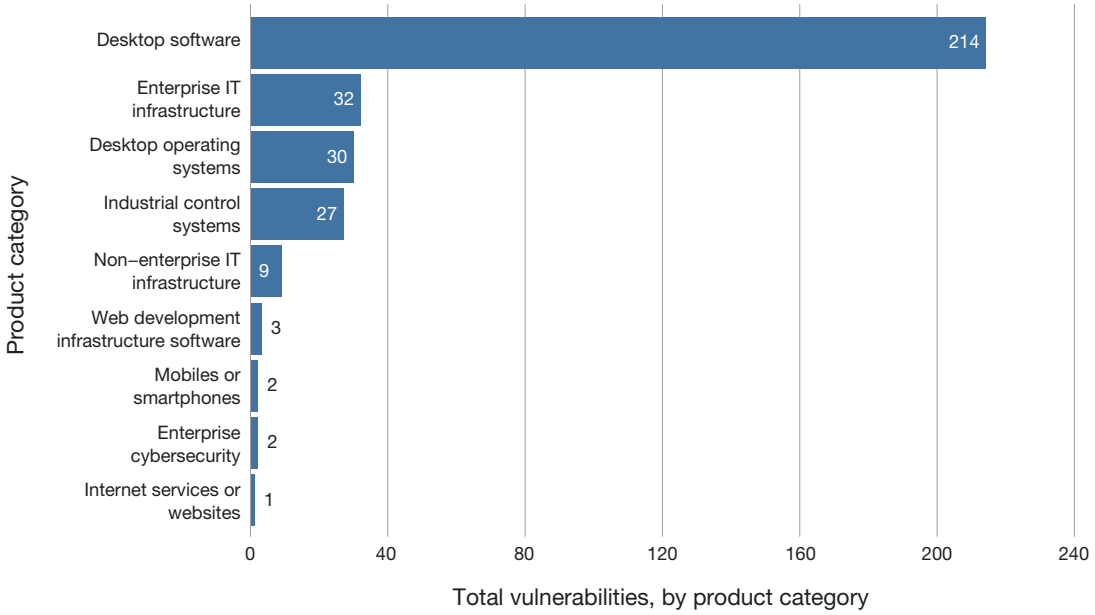
We would expect CVE DS 2 patch development times shown in Figure 11 to be shorter than CVE DS 1 operational times because CVE DS 2 uses the CVE discovery date as a starting point, and CVE DS 1 uses the previous major release date. This expectation is met, except in the case of mobile phone. Some CVE DS 1 data points had very short operational times, causing CVE DS 1 to be considerably shorter than CVE DS 2 on average (132 days versus 244 days, respectively).

Figure 11 shows the distribution of estimated patch development time by product category using CVE DS 2. *Patch development time* is the time from CVE discovery to the date that a patch addressing the CVE is released. This period represents the end portion of the operational time of a CVE and does not include the period from introduction to discovery. Patch development time was examined to explore trends across product categories in addition to total operational times. Patch development times appear to have similar ranges across product categories; mobiles and smartphones stand out for having the longest time between updates. It should be noted that the data shown have a limited number of entries for some product categories, specifically internet services and websites in CVE DS 2.

The product categories shown here are one method of attempting to group similar vulnerabilities, but this is not the only method available. Some datasets, such as Google Project Zero, classify vulnerabilities according to their effects rather than

FIGURE 8

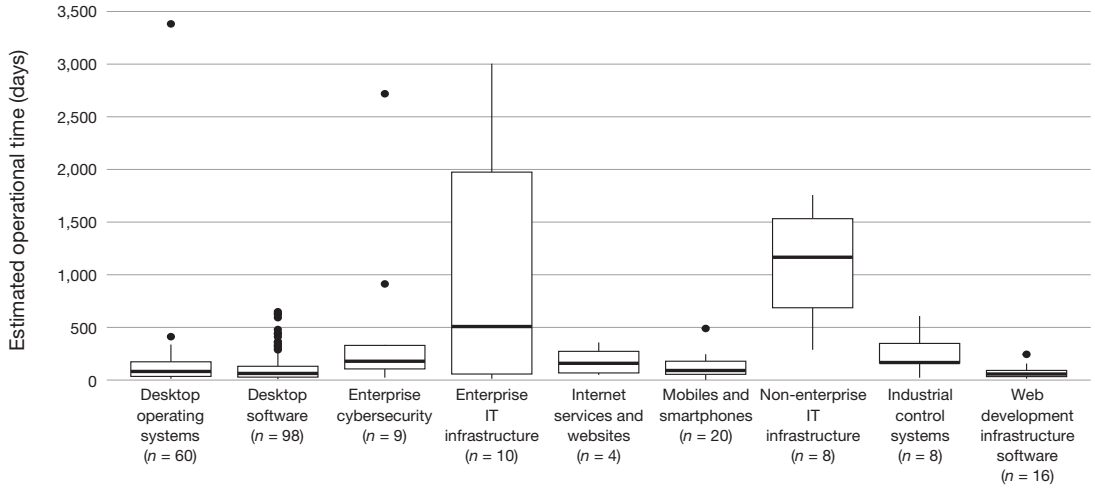
Vulnerability Count, by Product Category, for CVE DS 2



SOURCE: Authors' analysis of CVE DS2 data collected from Trend Micro Zero Day Initiative, undated. The data displayed constitute all vulnerabilities in CVE DS 2.

FIGURE 9

Estimated Operational Life Span for CVE DS 1



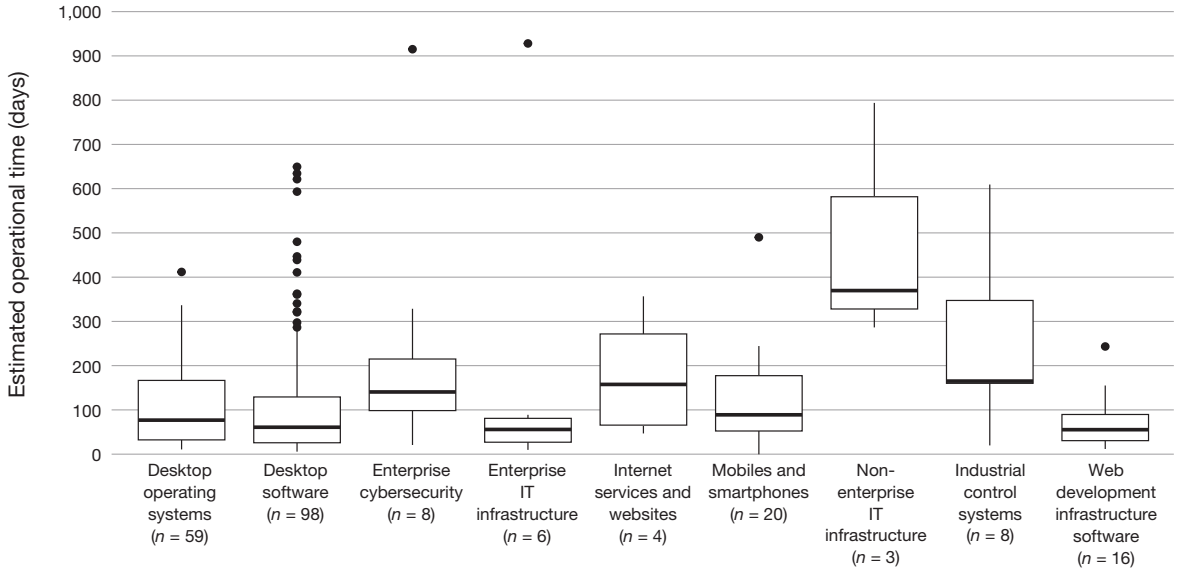
SOURCE: Authors' analysis of CVE DS 1 operational time data Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated.

NOTE: The box portion represents the first quartile, median, and third quartile of the data. The upper and lower whiskers extend, respectively, to the largest and smallest value within 1.5 times the interquartile range from the edge of the box.

the target environment. Additions to the size of the dataset shown or alternate methods of classifying vulnerabilities might provide different insight into the pattern of estimated operational times across vulnerabilities. The ranges of times shown in this report were used to inform distributions used in the exploratory simulation when estimating operational times. Table 2 shows the full data in tabular form.

FIGURE 10

Estimated Operational Life Span with Selected Data Removed for CVE DS 1



SOURCE: Authors' analysis of CVE DS 1 operational time data from Google, 2023; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated. Truncated data consist of four Microsoft Exchange servers, one Linux kernel, one Juniper firewall, and four NETGEAR home router vulnerabilities.

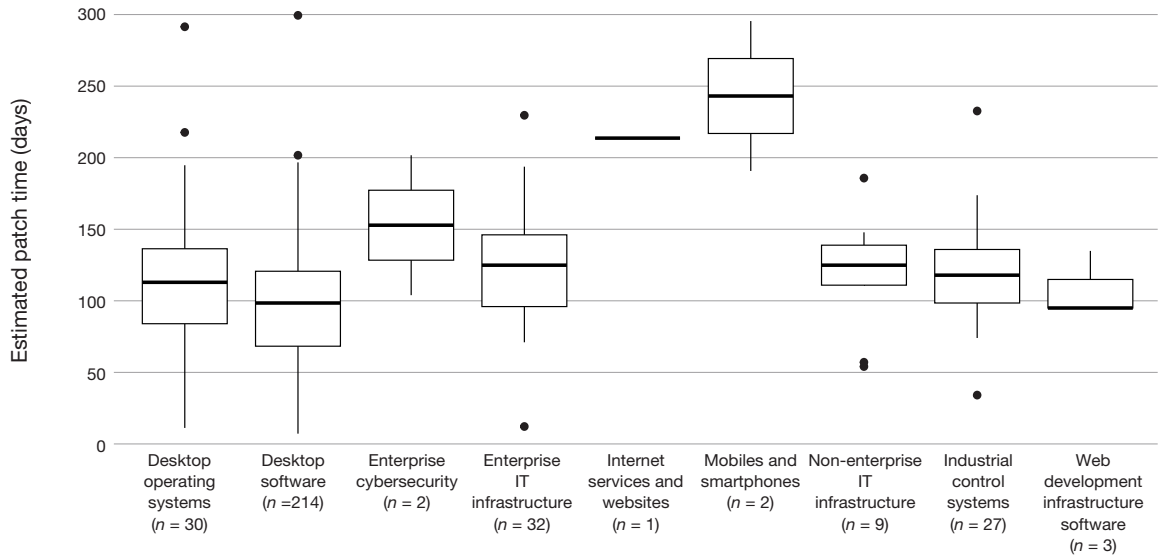
Most of the product categories appear to have similar operational time ranges, although there are a few obvious exceptions in enterprise IT infrastructure and non-enterprise IT infrastructure. A simple one-way analysis of variance comparing the means of all nine product categories (using the full data from Figure 9) found a statistically significant difference between means. This is unsurprising given the relatively long operational times for the IT infrastructure product categories relative to the other categories. To tease out where statistically significant differences exist between all categories, we used Tukey's range test for pairwise comparisons of product category means.[8] Figure 12 summarizes the results of the test showing the pairwise differences between group means.

Pairwise comparisons including 0 indicate that the means are not significantly different for $p > 0.05$. In the figure, pairwise comparisons in black do not have significantly different means, and those in red do have significantly different means. As expected from the box plot in Figure 8, any comparison including enterprise IT infrastructure and non-enterprise IT infrastructure had a significantly different mean from every other category. There are only two exceptions. The first is the comparison between both IT infrastructure categories, enterprise IT and non-enterprise IT. When comparing these two categories, the means were equivalent according to statistical significance. The other anomaly is that non-enterprise IT infrastructure and enterprise cybersecurity have statistically similar means, although the significance barely meets the $p > 0.05$ threshold. This result is surprising on first examination of Figures 8 and 9; however, both categories have relatively small counts in our database, and there are some significant outliers in the enterprise cybersecurity product category.

Given this analysis of the operational times in the vulnerability database, perhaps breaking out and distinguishing between the nine product categories as we have done in this initial report is not required. It does seem that, at a minimum, vulnerabilities associated with infrastructure, whether enterprise or non-enterprise IT, should be distinguished from the other product categories.[9]

FIGURE 11

Patch Development Time for CVE DS 2



SOURCE: Authors' analysis of CVE DS2 patch development time data from Trend Micro Zero Day Initiative, undated.

TABLE 2

Summary Data on Operational Times CVE DS 1

Product Category	Vulnerabilities	Minimum (days)	Median (days)	Mean (days)	Maximum (days)
Non-enterprise IT infrastructure (home networking equipment, internet of things)	8	288	1,169	1,078	1,761
Enterprise IT infrastructure (networking, routers, Wi-Fi, email browsers)	10	12	510	1,115	3,011
Enterprise cybersecurity (firewall)	9	23	179	516	2,725
Industrial control systems (SCADA)	8	22	167	268	610
Internet services and websites (Tor, Google search, VPN services)	4	49	160	182	358
Mobiles and smartphones (iOS, Android, mobile apps)	20	2	91	132	491
Desktop OSs (Windows, iOS, Linux)	60	13	82	165	3,390
Desktop software (plus web browsers)	98	8	63	126	650
Web development infrastructure software	16	14	58	73	245

NOTE: Users or operators of the vulnerable software might take time to apply patches after the patch release date. That time is not shown here.

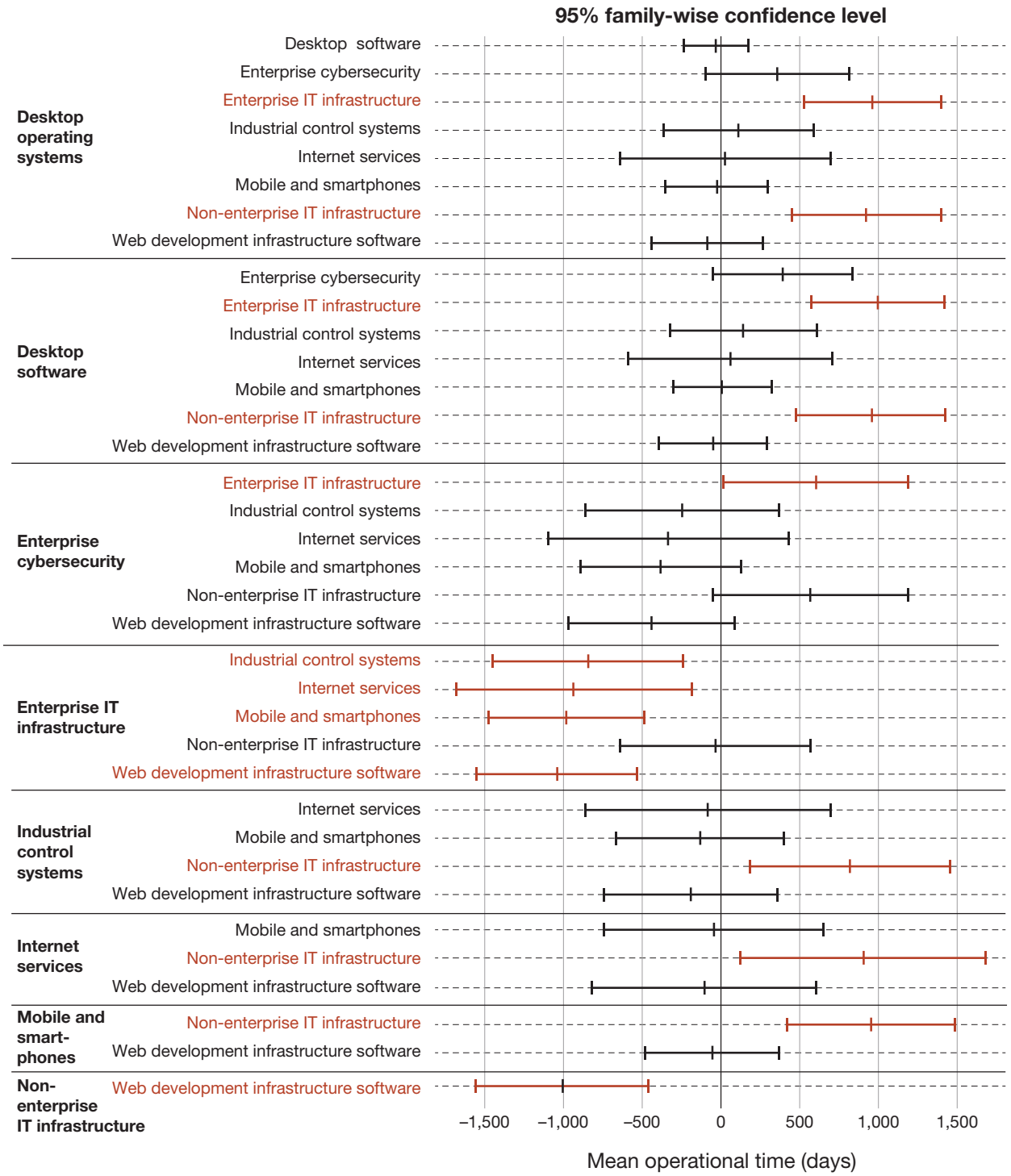
Software Update Cadence Analysis

Figure 13 shows a visual representation of two assumptions that can be used to estimate how long CVEs were active in the wild using the assembled software update cadence dataset—the time between major software releases or the time between minor software releases. Data are grouped by assigned product categories.

Figure 13 shows that significantly less time elapsed between releases for minor updates when generally compared with releases for major updates

FIGURE 12

Differences in Product Category Mean Operational Times



SOURCES: Authors' analysis of CVE DS 1 operational time data from Google, undated; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated.

NOTE: Pairwise comparisons in black do not have significantly different means. Pairwise comparisons in red do have significantly different means.

(as might be expected). Desktop operating systems take the longest time between major updates, while products in the desktop software category generally take less time between major updates. These ranges reflect only a subset of products because of the data limitations discussed, resulting in a small number of data points for certain product categories.

Next steps could include additional efforts to collect existing records of major and minor software updates. A more robust dataset could result in changes to the time ranges shown in Figure 13.

Simulating a Notional Joint Cyber Weapon Acquisition

During the prior analysis (Wilson et al., 2023), an exploratory model was created to estimate the lifespans of vulnerabilities and their associated costs to the Marine Corps in developing exploits, implants, and payloads associated with those vulnerabilities (Wilson et al., 2023).[10] That model was adjusted to simulate the nine product categories discussed previously, building on the previous options of desktop and mobile. Additionally, distributions for simulated operational lifespans that reflected the data discussed previously were created to attempt to quantify some of the uncertainty with real-world data.

We created a design of nine scenarios to illustrate the estimated impact on number of CCs operational and associated cost of investments over five fiscal years. In each investment scenario, 20 CCs that could be employed against a potential vulnerability are developed in each of the five years for a total of 100 CCs. There are three types of CCs in the investment scenarios. Exploits, implants, and payloads represent 75 percent, 15 percent, and 10 percent of CCs, respectively. The distinction of whether a CC is an exploit, implant, or payload in this model currently affects only the cost variable. Each CC was assigned one of the nine product categories. The proportion of product categories is reflective of the data collected in CVE DS 1; desktop software items are the most common, and internet services and website items are the least common.

Three sets of normal distributions were created to represent three assumptions of expected operational time using (1) the estimated operational times from the CVE DS 1, (2) the cadence of collected major software updates, and (3) the cadence of minor software updates. Each set of distributions has variations by product category, constructing a normal distribution for each using the associated mean and a standard deviation of one-third of the mean. The model makes a random draw over the specified distribution to simulate an operational time for each CC in an investment scenario. The possible combinations of three operational time assumptions and nine product categories used by the model are illustrated in Figure 14.

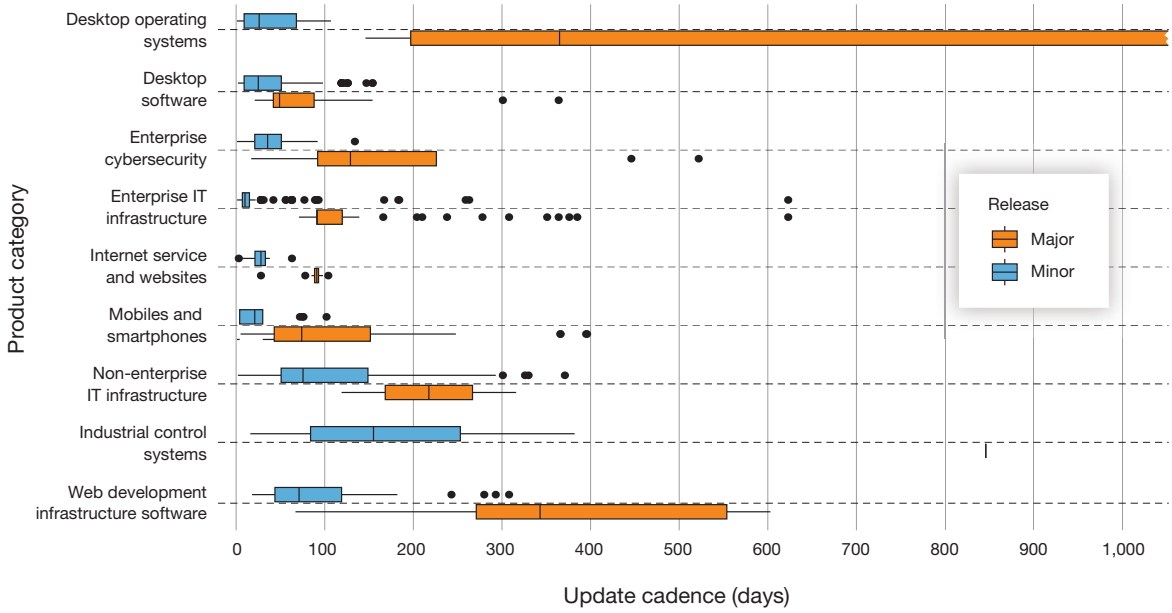
The three assumptions relating to operational time were combined with three levels of item complexity to create nine illustrative investment scenarios. The complexity variable in the model affects acquisition time and cost of a CC. Model parameters can be adjusted. It should be noted that the results shown are illustrative of assumptions that reflect the combined CVE data collected with the previously discussed caveats to data collection.

Scenarios were set up to explore the impact of variation in assumptions relating to both operational time and cost assumptions. Details of the main attributes defining each scenario are as follows:

- **CCs.** This attribute is the total number of CCs developed in the five-year scenario. For this experimental design, each scenario had an identical set-up of 20 CCs developed each year over a five-year period for a total of 100 CCs. A functionality of the model is the ability to replicate this baseline number of CCs any number of times as specified by the user to explore larger investment portfolios (i.e., develop 200, 300, etc. over the five-year simulation period).
- **Exploit-implant-payload proportion.** Each CC developed is designated as an exploit, implant, or payload. The distinction affects cost but does not affect operational time. In each scenario, an identical setup is used in which the proportions of CCs that are exploits, implants, and payloads are 75 percent, 15 percent, and 10 percent, respectively.

FIGURE 13

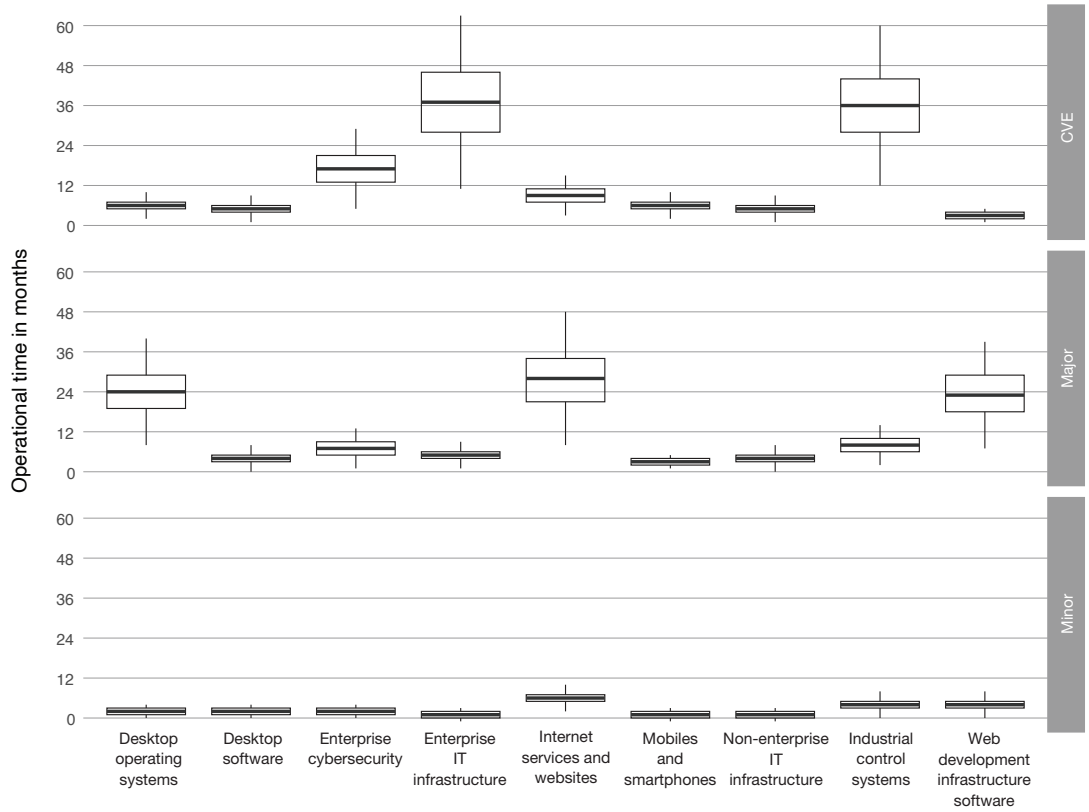
Software Update Cadence Data, by Product Category



SOURCE: Authors' analysis of open-source data listed in Table A.1.

FIGURE 14

Model Operational Time Distributions, by Product Category



- **Operational time distribution data.** Each scenario uses a set of distributions to simulate operational times of CCs reflective of one of three assumptions. The distributions used for simulated operational times are informed by (1) CVE DS 1 data, (2) major update cadence data, or (3) minor update cadence data.
- **Complexity.** To abstractly capture the variability in research and development costs, a simple ranking of low, medium, and high complexity is assigned to each CC in a scenario. A higher complexity is associated with a higher cost and a longer period of acquisition preceding the start of operational time in the model.
- **Operational Capability Threshold.** This value serves as an example mission requirement that an investment scenario aims to achieve at minimum. For each scenario, the baseline investment plan can be replicated until the conditions in which the Operational Capability Threshold are met consistently. For each scenario modeled, we used a simple assumption that the goal is to have at least five CCs of any type operational at all times.
- **Operational Capability Objective.** While the Operational Capability Threshold represents a **minimum** value to achieve, the Operational Capability Objective represents the **desired** outcome of investments. We used the simple assumption of an Operational Capability Objective of at least ten operational CCs of any type at all times. Displaying both the threshold and objective values on model result charts can be useful for visually assessing how well an example scenario meets mission requirements.

Table 3 summarizes the simulated investment scenarios, and Figure 14 shows a visual representation of the simulated operational time distributions used in the model, by product category and under three operational time assumptions. Results in this section are from the model running 100 iterations of each scenario.

The y-axis represents the likelihood and range of simulated operational times assigned to a CC in the model, and the x-axis shows variability across the nine product categories. The three options for operational time distribution assumptions are shown. For example, the product category of desktop operating systems using the major update distribution has a 50 percent likelihood of the model assigning an operational time of approximately 18 to 30 months. Normal distributions that represent the potential operational time of

TABLE 3
Design of Experiments

Scenario	CCs	Exploit-Implant-Payload Proportion	Operational Time Distribution Data	Complexity	Operational Capability Threshold	Operational Capability Objective
1	100	75%-15%-10%	CVE DS 1	High	5	10
2	100	75%-15%-10%	CVE DS 1	Medium	5	10
3	100	75%-15%-10%	CVE DS 1	Low	5	10
4	100	75%-15%-10%	Major updates	High	5	10
5	100	75%-15%-10%	Major updates	Medium	5	10
6	100	75%-15%-10%	Major updates	Low	5	10
7	100	75%-15%-10%	Minor updates	High	5	10
8	100	75%-15%-10%	Minor updates	Medium	5	10
9	100	75%-15%-10%	Minor updates	Low	5	10

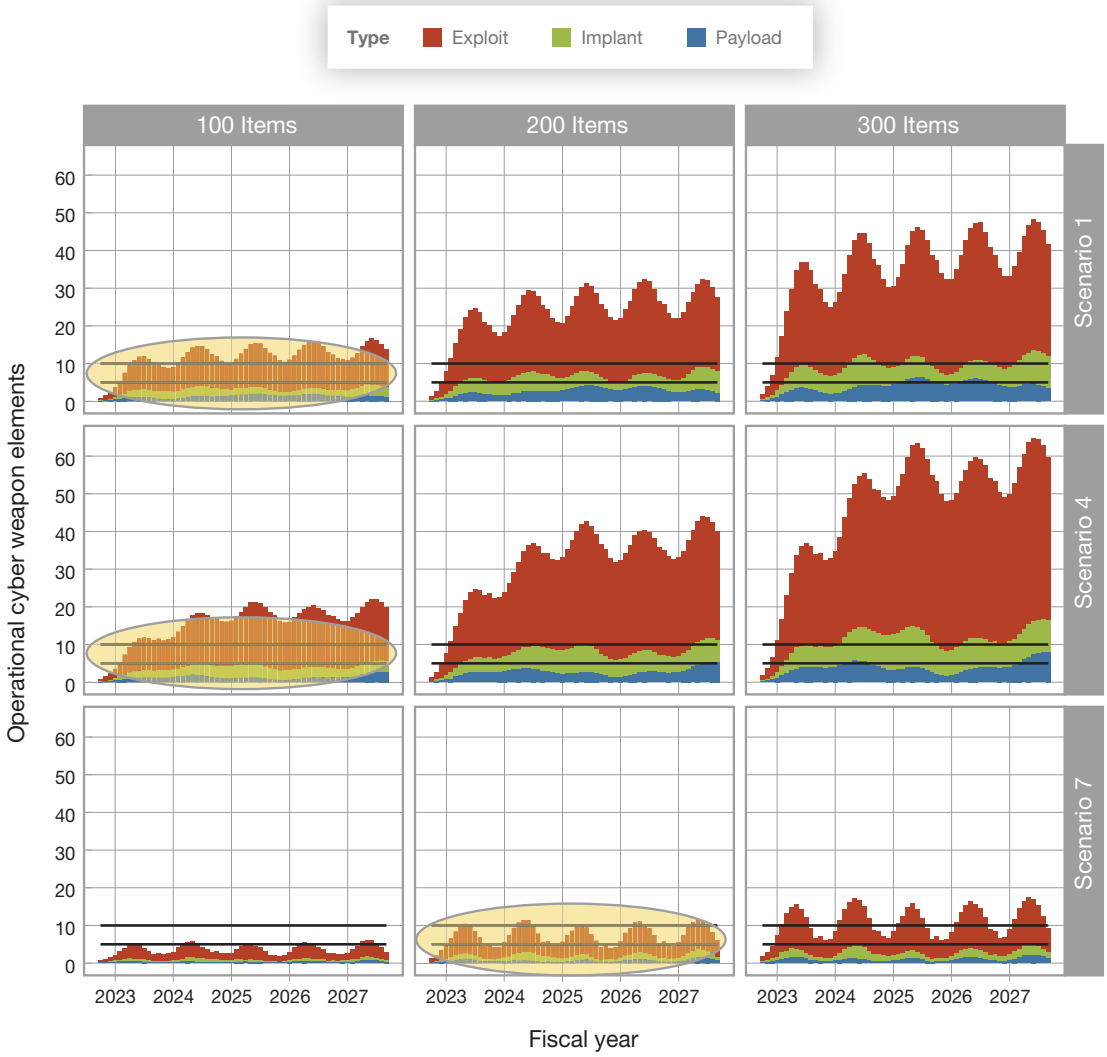
NOTE: For each scenario, 100 items represent the starting baseline investment portfolio. Adjustments to the baseline investment portfolio for each scenario to meet the Operational Capability Threshold were identified and selected when displaying estimated program costs. Scenarios 7 to 9 required an expanded investment portfolio to meet the operational threshold.

each product category were created using the mean operational time of the respective product category in the associated dataset. The variations in simulated product category operational time ranges reflect the analysis of CVE DS 1, major software update cadence, and minor software update cadence datasets. The model then randomly draws from those distributions to simulate operational times.

In Figure 15, we show three scenarios (1, 4, and 7) that have been replicated by the model to show investment portfolios of 100, 200, and 300 CCs over five years. All three scenarios assume high item complexity. Horizontal black lines represent the Operational Capability Threshold (five operational CCs) and Operational Capability Objective (ten operational CCs) of the scenario. The estimated number of all operational CCs over time are displayed as stacked bars to assess whether the example mission-objective has been satisfied. Scenario 1 represents the simulated operational times informed by CVE DS 1, while Scenario 4 and Scenario 7 represent simulated operational times informed by the cadence of major software updates and the cadence of minor software updates, respectively. Each scenario has uniform CC

FIGURE 15

Meeting a Notional Mission Requirement in High-Complexity Scenarios



NOTE: The circled chart indicates the investment portfolio (number of cyber weapons) that needs to be procured at any given time to meet the threshold.

investments across the five years of the simulation, which results in the periodic nature observed.

The model allows the user to replicate the baseline investment of CCs to assess how many CCs might be operational over time under a set of model assumptions. For each scenario, we attempted to identify the portfolio that would meet a threshold of five operational CCs at any time with an objective of ten operational CCs.

Horizontal lines represent the threshold and objective levels. The assumptions behind simulated operational time distributions in both Scenario 1 and Scenario 4 contain the potential for operational times of a year or more. The result of this impact leads to increased peaks values because investments from previous years are still operational as new investments come to fruition. Scenario 7, using the cadence of minor software updates to estimate operational lifespans, represents a worst-case scenario that would force tight timelines on the JCW program. In this case, JCW would need to procure twice the number of originally planned investments to meet the threshold of at least five operational capabilities at any time over the five-year period.

To estimate the cost of CC operationalization, we used publicly available bounty payouts for zero-day exploits provided by Zerodium as assumed total costs, which are grouped into price ceilings ranging from $10,000 to $2,500,000. To pair this cost range with the complexity model attribute capturing cost variability, we associated low-, medium-, and high-complexity exploit costs with quartile one, two, and three of the Zerodium cost range, respectively. We used an assumption that implants need at least four times the resources to develop compared with exploits, while payload development uses one-quarter fewer resources relative to exploit development.[11] Table 4 summarizes the costs used for analysis. It should be noted that these costs represent rough order-of-magnitude estimates to demonstrate model proof of concept.

Figure 16 shows the estimated program costs of the nine scenarios using the base CC costs displayed in Table 4. Further detail of how costs are simulated within the model, including apportioning of acquisition and operations and maintenance costs, can be found in the companion document of prior analysis (Wilson et al., 2023).

The model input that represents complexity has a large impact on the total estimated cost when other model parameters are held constant. Using simulated operational times informed by the collected CVE data creates comparable model outputs to scenarios that simulate operational times informed by the cadence of major collected software updates. Notably, the last three scenarios with operational times informed by the cadence of minor collected software updates have higher comparative costs. These higher costs are because of the shorter assumed operational times, fewer resulting months of operational capability, and a larger investment portfolio required to meet the notional mission requirement.

Conclusions

A novel dataset of publicly tracked CVEs was assembled and then used to estimate operational times by computing the time between the last major update of a specific software and the patch date listed. Software

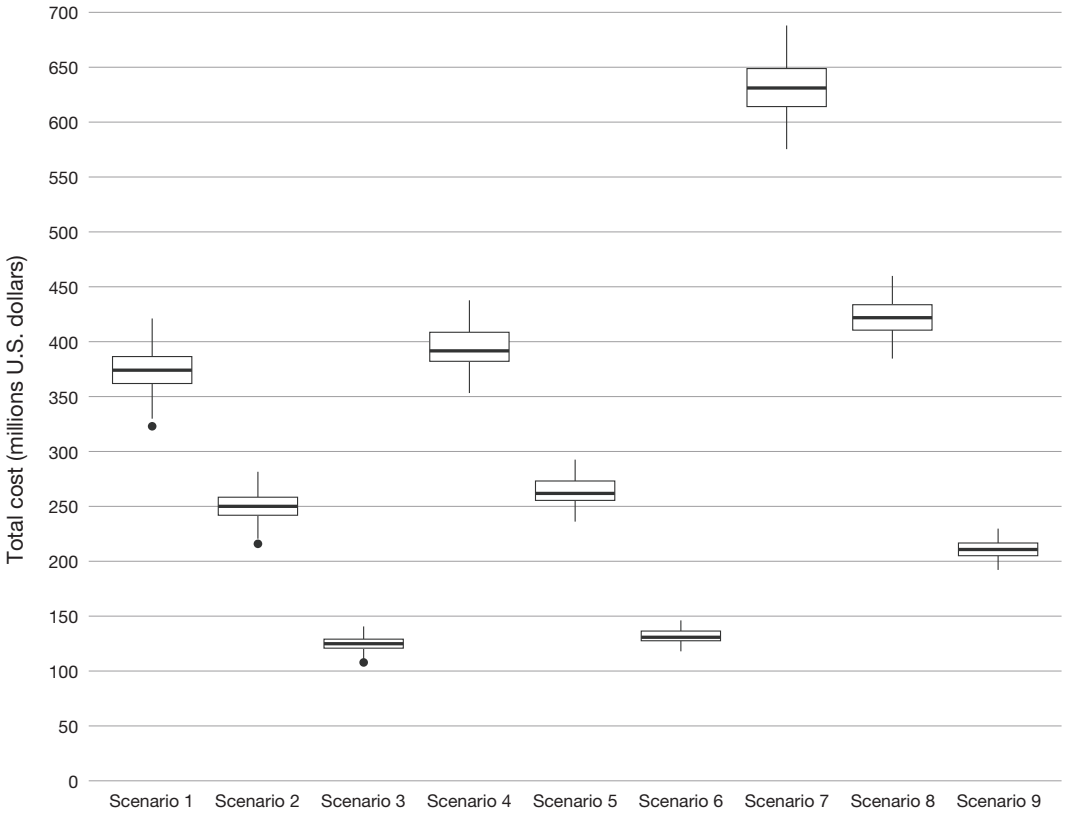
TABLE 4
Cyber Capability Complexity Costs

	Total CC Cost (U.S. Dollars)		
CC Type	Low	Medium	High
Exploit	632.5	1,255.0	1,877.5
Implant	2,530.0	5,020.0	7,510.0
Payload	474.4	941.3	1,408.1

SOURCE: Features exploit bounty payout data adjusted to account for cost differences in operationalizing implants and payloads from Zerodium, undated.

NOTE: Amounts in thousands of base year 2023 dollars.

FIGURE 16
Investment Portfolio Total Cost



NOTE: For Scenarios 7–9, with the update cadence of minor software updates, 200 items were required in the investment portfolio to achieve the notional mission requirement of at least five operational CCs at any time.

update cadence data were also collected and used to explore potential trends across a variety of product categories. Altogether, the operational time data were used to estimate the range of possible life-cycle costs of the JCW program, which are subject to considerable uncertainty.

The estimated range of cost for the JCW program across scenario one through six span from approximately $125 million to $375 million, which is wider than the $90 million to $275 million range found in the first study (Wilson et al., 2023). Scenario seven illustrates how assumptions of highest complexity and lowest operational time may increase the cost estimate to approximately $625 million. A key assumption involves procuring enough active cyber weapons to maintain a notional threshold of five operational cyber capabilities. The cost and time to develop an offensive cyber weapon capability also has uncertainty because of the varying operational times of vulnerabilities that the weapons exploit and their associated complexity.

Two categories, software enterprise IT infrastructure and non-enterprise IT infrastructure, had longer historic average vulnerability operational times than other software categories that use collected CVE data (1,115 and 1,078 average days, respectively) and could be expected to be less costly to develop exploits for as a result. The dataset assembled had a relatively small number of items in these two product categories, and expansion of the dataset could change this result.

Vulnerabilities across all nine product categories display a range of minor software update frequencies from an average of 20 days for mobile and smartphones to 178 days for industrial control systems, which can be used as a proxy to estimate operational time.

Open-source data collection of vulnerabilities and CVEs presents challenges. Certain attributes, such as the vendor and product affected by a vulnerability, are commonly tracked, but variables related to time, such as the introduction, discovery, and patch date, are less uniformly documented. Without an obvious automation approach, doing so requires time-consuming manual effort to identify information on relevant vulnerabilities. Automation of data collection could be an option but presents challenges of its own, such as generalizing code for unclean and sometimes unstructured data.

Open-source data are weighted toward common types of software. As less common types of software are sought, the difficulty of finding comparable data points increases.

APPENDIX

List of Vendors and Sources

This appendix details the full list of vendors and products used in the analysis. Table A.1 lists the vendor, product, and source information used to create the software update cadence data.

Table A.2 lists the vendor, product, and CVE source used to create CVE DS 1.

Table A.3 lists the vendors and products from the expanded Trend Micro analysis used to create CVE DS 2.

TABLE A.1
Vendors, Products, and Sources for Update Cadence Data

Vendor	Product	Source	Last Visited
Adobe	Flash	Adobe, 2020	February 7, 2023
Adobe	Reader	Adobe, 2023	February 7, 2023
Apple	iOS	Apple, undated-a	February 7, 2023
Apple	MacOS	Apple, undated-b	February 7, 2023
ARM	Android	Android Source, 2021	February 7, 2023
Delta Industrial Automation	CNCSoft	Delta Industrial Automation, undated-a	February 7, 2023
Delta Industrial Automation	DOPSoft	Delta Industrial Automation, undated-b	February 7, 2023
Ecava	Integraxor	Ecava, undated	February 7, 2023
Facebook	WhatsApp	Older versions of WhatsApp Messenger (Android)	February 7, 2023
Google	Android	Google, undated	February 7, 2023
Google	Chrome	Google, 2023	February 7, 2023
ICONICS	Genesis64	Iconics, undated	February 7, 2023
Linux	Kernel	LiLinux, 2023	February 7, 2023
Microsoft	Exchange Server 2019, 2016, 2013	Microsoft, 2023a	February 7, 2023
Microsoft	Internet Explorer 11	Microsoft, undated-a	February 7, 2023
Microsoft	Office	Microsoft, 2023c	February 7, 2023
Microsoft	Silverlight	Microsoft, undated-b	February 7, 2023
Microsoft	Windows 10	Microsoft, 2023b	February 7, 2023
NETGEAR	R6260	NETGEAR, undated-a	February 7, 2023

Table A.1—Continued

Vendor	Product	Source	Last Visited
NETGEAR	R6700v3	NETGEAR, undated-b	February 7, 2023
NETGEAR	R7000	NETGEAR, undated-c	February 7, 2023
NETGEAR	R7800	NETGEAR, undated-d	February 7, 2023
Qualcomm	Android	Qualcomm, 2021	February 7, 2023
Sophos	Firewall Software	Sophos, undated	February 7, 2023
VMWare	Identity Manager	VMware, 2023	February 7, 2023
VMWare	Workspace ONE Access	VMware, 2021	February 7, 2023
Zone Alarm	Extreme Security Next Gen	ZoneAlarm, undated	February 7, 2023

NOTE: The dataset gathered is limited to vendors and products for which update version and date information could be identified during a manual search process.

TABLE A.2
Vendors and Products in CVE DS 1 Operational Time Data

Vendor	Product	Source
Adobe	Flash	Google Project Zero
Adobe	Reader	Google Project Zero
Apache	Struts	Zero Day Project
Apple	WebKit	Google Project Zero
Apple	iOS	Google Project Zero
Apple	iOS	Zero Day Project
Apple	macOS	Zero Day Project
ARM	Android	Google Project Zero
Check Point	ZoneAlarm	Trend Micro
Cisco	ASA	Google Project Zero
Cisco	IOS XR	Zero Day Project
D-Link	DAP-1860	Trend Micro
Delta Industrial Automation	CNCSoft ScreenEditor	Trend Micro
Delta Industrial Automation	CNCSoft-B	Trend Micro
Delta Industrial Automation	CNCSoft-B DOPSoft	Trend Micro
Delta Industrial Automation	DOPSoft	Trend Micro
Drupal	Drupal core	Zero Day Project
Facebook	WhatsApp	Google Project Zero
Fancy Product Designer	Fancy Product Designer	Zero Day Project
FreeBSD	Kernel	Trend Micro
Ghostscript	Ghostscript	Google Project Zero

Table A.2—Continued

Vendor	Product	Source
Google	Chrome	Google Project Zero
Google	Chrome	Zero Day Project
Google	Android	Google Project Zero
ICONICS	GENESIS64	Trend Micro
Jenkins	Jenkins	Zero Day Project
Juniper	Network and Security Manager	Trend Micro
Linux	Kernel	Zero Day Project
Linux	Kernel	Google Project Zero
Matrix.org	Synapse	Zero Day Project
Microsoft	Edge	Zero Day Project
Microsoft	Windows	Google Project Zero
Microsoft	Windows	Zero Day Project
Microsoft	Office	Google Project Zero
Microsoft	Internet Explorer	Google Project Zero
Microsoft	VBScript	Google Project Zero
Microsoft	Windows Kernel	Google Project Zero
Microsoft	Silverlight	Google Project Zero
Microsoft	Exchange Server	Google Project Zero
Mozilla	Firefox	Google Project Zero
NETGEAR	R7000	Trend Micro
NETGEAR	R6700v3	Trend Micro
NETGEAR	R6260	Trend Micro
NETGEAR	R7800	Trend Micro
Open Information Security Foundation	Suricata	Zero Day Project
Open Source Matters, Inc.	Joomla!	Zero Day Project
Oracle	Solaris	Zero Day Project
Oracle	Java	Google Project Zero
Pivotal Software	Spring Framework	Zero Day Project
Qualcomm	Android	Google Project Zero
Roundcube	Roundcube webmail	Zero Day Project
SolarWinds	Serv-U FTP Server	Zero Day Project
SolarWinds	Orion API	Zero Day Project
SonicWall	SMA 100	Zero Day Project
Sophos	XG Firewall	Zero Day Project

Table A.2—Continued

Vendor	Product	Source
Sophos	XG Firewall	Google Project Zero
Trend Micro	Apex One	Zero Day Project
TYPO3	TYPO3	Zero Day Project
VMware	Workspace ONE Access	Google Project Zero
Warefare Plugins	Social Warfare plugin	Zero Day Project
WordPress	File Manager	Zero Day Project
Zimbra Collaborartion	Zimbra	Zero Day Project
Zoho	ManageEngine ADSelfservice Plus	Zero Day Project

SOURCES: Google, undated; Trend Micro Zero Day Initiative, undated; and Zero-Day Tracking Project, undated.

NOTE: CVE that were selected for the combined dataset range from 2014 to 2022. Additionally, only vulnerabilities with an identified patch date were included to allow for operational time estimation.

TABLE A.3

Vendors and Products in CVE DS 2 Patch Development Time Data

Vendor	Product
ABB	Panel Builder 800
Adobe	Acrobat Pro DC
Adobe	Acrobat Reader DC
Adobe	After Effects
Adobe	Bridge
Adobe	Flash
Adobe	Flash Player
Adobe	FrameMaker
Adobe	Illustrator
Adobe	InCopy
Adobe	InDesign
Adobe	Media Encoder
Adobe	Photoshop
Adobe	Prelude
Adobe	Reader
Adobe	Reader DC
Advantech	Advantech WebAccess
Advantech	iView
Advantech	WebAccess
Advantech	WebAccess Node

Table A.3—Continued

Vendor	Product
Advantech	WebAccess/HMI Designer
Advantech	WebAccess/NMS
Advantech	WebAccess/SCADA
AlienVault	OSSIM
Apple	macOS
Apple	OS X
Apple	QuickTime
Apple	Safari
Autodesk	AutoCAD
Autodesk	Design Review
Autodesk	FBX Review
Autodesk	Navisworks Freedom
Autodesk	Navisworks Manage
AVEVA	Edge
Bentley	MicroStation CONNECT
Bentley	View
Bosch	B426
Canonical	Ubuntu
Cisco	Data Center Network Manager
Cisco	Prime Collaboration Provisioning
Cisco	UCS Director
Cisco	WebEx
Crestron	TSW-760
D-Link	DAP-1860
D-Link	Multiple Routers
Delta Industrial Automation	CNCSoft
Delta Industrial Automation	CNCSoft ScreenEditor
Delta Industrial Automation	CNCSoft-B
Delta Industrial Automation	CNCSoft-B DOPSoft
Delta Industrial Automation	DIAScreen
Delta Industrial Automation	DOPSoft
Drupal	Drupal 8
Eaton	HMiSoft

Table A.3—Continued

Vendor	Product
Ecava	IntegraXor
Fatek Automation	WinProladder
Foxit	Foxit PDF SDK DLL
Foxit	PDF Editor
Foxit	PDF Reader
Foxit	PhantomPDF
Foxit	Reader
Foxit	Studio Photo
FreeBSD	Kernel
Google	Android
IBM	Spectrum Protect Plus
ICONICS	GENESIS64
Intel Security	True Key
Kaspersky	Total Security
McAfee	Total Protection
NETGEAR	R6260
NETGEAR	R6700v3
NETGEAR	R7000
NETGEAR	R7800
Parallels	Access
SolarWinds	Network Performance Monitor
SolarWinds	Orion Network Performance Monitor
VMware	ESXi
VMware	vCenter Server Appliance
VMware	VMware Workstation
VMware	Workstation
X.Org	Server

Notes

[1] U.S. Marine Corps Systems Command's (MARCORSYSCOM's) Joint Cyber Weapons (JCW) acquisition program provides advanced cyber warfare capabilities to support U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER), U.S. Cyber Command (USCYBERCOM), combatant commanders, and other federal government agencies' global operations; Acquisition artifacts include an Acquisition Strategy, Capability Needs Statement, Cybersecurity Strategy, Information Support Plan, Intellectual Property Strategy, Lifecycle Cost Estimate, Product Support Strategy, Test Strategy, and User Agreement.

[2] These were interchangeably referred to as cyber weapon elements in the companion research.

[3] A zero day exploit takes advantage of a software vulnerability that has not yet been publicly identified or patched.

[4] The other five areas of potential enhancement identified in Wilson et al. (2023) were (1) incorporating historical data on cyber capabilities, (2) increasing the granularity of exploit types, (3) characterizing the acquisition type for the exploit, (4) incorporating additional cost and schedule drivers, and (5) converting the exploratory simulation into an optimization model.

[5] Given an example version 1.2, we assume that the most recent major update prior to 1.2 (i.e., 1.0) is the earliest affected version.

[6] Zerodium lists the eight product categories as clients/files, email servers, mobiles/smartphones, operating systems, research/techniques, web apps/panels, web browsers, web servers (Zerodium, undated).

[7] These data are shown in detail in Figure 13.

[8] We used the TukeyHSD test in R to conduct the analysis.

[9] Specifically, the product categories enterprise IT infrastructure and non-enterprise IT infrastructure from the product category description list should be distinguished from other categories.

[10] An *exploit* is "[a] technique to breach the security of a network or information system in violation of security policy" (National Initiative for Cybersecurity Careers and Studies, 2023). An *implant* is "a program that solidifies and maintains access initially provided by an exploit (i.e., achieves persistence) and delivers some effect to the system" (Ablon and Bogart, 2017). A *payload* is a CC that accomplishes the intended goal of the cyber weapon (Bellovin, Landau, and Lin, 2017).

[11] Discussion with JCW Program Office on JCW historical data and experience, May 2021.

References

Ablon, Lillian, and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, RR-1751-RC, 2017. As of August 3, 2023: https://www.rand.org/pubs/research_reports/RR1751.html

Adobe, "Release Notes for Flash Player 32 and AIR 32," webpage, December 8, 2020. As of August 3, 2023: https://helpx.adobe.com/flash-player/release-note/fp_32_air_32_release_notes.html

Adobe, "Release Notes Acrobat, Reader," webpage, last updated July 11, 2023. As of August 3, 2023: https://helpx.adobe.com/acrobat/release-note/release-notes-acrobat-reader.html

Android Source, "Android 10 Security Release Notes," webpage, last updated January 27, 2021. As of August 3, 2023: https://source.android.com/docs/security/bulletin/android-10

Android Source, "Android 13 and Android 13 QPR Release Notes," webpage, undated. As of August 3, 2023: https://source.android.com/docs/setup/about/android-13-release

Apple, "iOS & iPadOS Release Notes," webpage, undated-a. As of August 3, 2023: https://developer.apple.com/documentation/ios-ipados-release-notes

Apple, "macOS Ventura 13.2 Release Notes," webpage, undated-b. As of August 3, 2023: https://developer.apple.com/documentation/macos-release-notes/macos-13_2-release-notes

Bellovin, Steven M., Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity*, Vol. 3, No. 1, March 2017.

Common Vulnerabilities and Exposures Program, MITRE Corporation, homepage, undated. As of August 3, 2023: https://cve.mitre.org/

Delta Industrial Automation, "CNCSoft V1.01.34 A Category: Industrial Automation/CNC Solution," webpage, undated-a. As of August 3, 2023: https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft%20V1.01.34&sort_expr=cdate&sort_dir=DESC

Delta Industrial Automation, "DOPSoft, Category: Industrial Automation / Touch Panel HMI - Human Machine Interfaces," webpage, undated-b. As of August 3, 2023: https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=DOPSoft%20&sort_expr=cdate&sort_dir=DESC

Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway*, October 2, 2020.

Google, "0day 'In the Wild,'" spreadsheet, last updated April 20, 2023. As of August 3, 2023: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=0

Ecava, "Integraxor Release Note," webpage, undated. As of August 3, 2023: https://www.integraxor.com/category/news/release/

Facebook WhatsApp, "WhatsApp Messenger," webpage, undated. As of August 3, 2023: https://whatsapp-messenger.en.uptodown.com/android/versions

Google, "Android 13 and Android 13 QPR Release Notes," webpage, undated. As of February 15, 2023: https://source.android.com/docs/setup/about/android-13-release

Google, "Chrome Dev for Android Update," *Google Blog*, February 15, 2023. As of August 3, 2023: https://chromereleases.googleblog.com/

Iconics, "Release Notes Iconics Suite," webpage, undated. As of August 3, 2023: https://docs.iconics.com/V10.97/GENESIS64/Help/Com/Intro/Release_Notes.htm

Linux, "KernelNewbies: LinuxVersions," webpage, last updated May 9, 2023. As of August 3, 2023: https://kernelnewbies.org/LinuxVersions

Microsoft, "Internet Explorer 11 Cumulative Update," webpage, undated-a. As of August 3, 2023: https://www.catalog.update.microsoft.com/Search.aspx?q=internet+explorer+11+cumulative+update

Microsoft, "Microsoft Silverlight Release History," webpage, undated-b. As of August 3, 2023: https://www.microsoft.com/getsilverlight/locale/en-us/html/Microsoft%20Silverlight%20Release%20History.htm

Microsoft, "Exchange Server Build Numbers and Release Dates," webpage, March 13, 2023a. As of August 3, 2023: https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2016

Microsoft, "Windows 10 Release Information," webpage, July 11, 2023b. As of August 3, 2023: https://learn.microsoft.com/en-us/windows/release-health/release-information

Microsoft, "Update History for Microsoft 365 Apps (Listed By Date)," webpage, July 31, 2023c. As of August 3, 2023: https://learn.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date

National Initiative for Cybersecurity Careers and Studies, "Glossary—Explore Terms: A Glossary of Common Cybersecurity Words and Phrases," webpage, last updated March 16, 2023. As of August 3, 2023: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

National Institute of Standards and Technology, "General Information," webpage, undated. As of August 3, 2023: https://nvd.nist.gov/general

Netgear, "R6260 — AC1600 Smart WiFi Router Dual Band Gigabit," webpage, undated-a. As of August 3, 2023: https://www.netgear.com/support/product/R6260.aspx#download

Netgear, "R6700 — Nighthawk AC1750 Smart WiFi Dual Band Gigabit Router" webpage, undated-b. As of August 3, 2023: https://www.netgear.com/support/product/r6700.aspx#download

Netgear, "R7000 — Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router," webpage, undated-c. As of August 3, 2023: https://www.netgear.com/support/product/r7000.aspx#download

Netgear, "R7800 — Nighthawk X4S AC2600 Smart WiFi Router," webpage, undated-d. As of August 3, 2023: https://www.netgear.com/support/product/R7800#download

Qualcomm, "Android 10 Security Release Notes," webpage, January 27, 2021. As of August 3, 2023: https://source.android.com/docs/security/bulletin/android-10

Sophos, "Sophos Release Notes," webpage, undated. As of August 3, 2023: https://docs.sophos.com/releasenotes/index.html?productGroupID= nsg&productID=xg&versionID=19.5

Trend Micro Zero Day Initiative, "Published Advisories" webpage, undated. As of August 3, 2023: https://www.zerodayinitiative.com/advisories/published/

VMware, "VMware Workspace ONE Access Cloud Release Notes," webpage, last updated November 3, 2021. As of August 3, 2023: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/rn/Workspace-ONE-Access-Cloud-2021-release-notes.html

VMware, "VMware Workspace ONE UEM Release Notes," webpage, last updated May 31, 2023. As of August 3, 2023: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/rn/Workspace-ONE-Product.html

Wilson, Bradley, Thomas Goughnour, Megan McKernan, Andrew Karode, Devin Tierney, Mark V. Arena, Michael J. D. Vermeer, Hansell Perez, and Alexis Levedahl, *A Cost Estimating Framework for U.S. Marine Corps Joint Cyber Weapons,* RAND Corporation, RR-A1124-1, 2023. As of August 3, 2023: https://www.rand.org/pubs/research_reports/RRA1124-1.html

Zero-Day Tracking Project, Zero-Day Vulnerability Database, database, undated. As of August 3, 2023: https://www.zero-day.cz/database/

Zerodium, "Zerodium Exploit Acquisition Program," webpage, undated. As of August 3, 2023: https://zerodium.com/program.html

ZoneAlarm, "Release History: ZoneAlarm Extreme Security NextGen," webpage, undated. As of August 3, 2023: https://www.zonealarm.com/software/extreme-security-nextgen/release-history

About This Report

U.S. Marine Corps Systems Command's Joint Cyber Weapons (JCW) acquisition program provides advanced cyber warfare capabilities to support U.S. Marine Corps Forces Cyberspace Command, U.S. Cyber Command, combatant commanders, and other federal government agencies' global operations. This report quantifies uncertainties related to cost and operational time of software vulnerabilities and provides an updated cost model for the JCW program. This analysis builds on *A Cost Estimating Framework for U.S. Marine Corps Joint Cyber Weapons* by incorporating data from additional vulnerability data sets that are combined to create a novel dataset for analysis of vulnerability lifespans (Wilson et al., 2023). The previous cost model was updated with these new data. We then explored potential investment portfolios.

The research reported here was completed in July 2023 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by U.S. Marine Corps Systems Command and conducted within the Navy and Marine Forces Program of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development program sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Navy and Marine Forces Program, see www.rand.org/nsrd/nmf or contact the director (contact information is on the webpage).

Acknowledgments

We thank David Pasquill, Product Manager, Program Management Office, Marine Corps Cyberspace Operations, for his guidance and insight during the development of the Software Acquisition Pathway documents described in this report. We also thank Col Thomas Dono, Major Matthew Gurrister, Torrence Moore, Vincent Monroe, Jermaine Kendall, and Nichole Sillaman who provided valuable support to this effort.

We thank Tim Conley and Sasha Romanosky for their constructive and thorough reviews of this analysis. Finally, Paul DeLuca and Brendan Toland, Director and Associate Director, respectively, of the Navy and Marine Forces Program, provided valuable guidance, and insightful comments on the research.

www.rand.org