Ground Zero: An In-Depth Analysis of 2022's Zero-Day Vulnerabilities

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA

Abstract: ***A zero - day vulnerability is a vulnerability in software or hardware that is typically unknown to the vendor and there is no patch or fix is available. Zero - day vulnerabilities present a significant challenge to an organization's cyber defense team. In 2022, the quantity of Zero - Day exploits significantly reduced compared to 2021. Zero days are still actively pursued by cybercriminal groups; they either actively find these vulnerabilities or buy them from the dark web. This article presents a thorough review of the Zero - Day vulnerabilities identified and exploited in 2022. This study analyzes trends, attack vectors, and the top targeted software platforms using public data sources such as Google's Threat Analysis Group (TAG), MITRE's CVE database, and Zero - Day. cz. A statistical analysis is performed to find trends and patterns. This study aims to offer insights from the zero - day vulnerabilities exploited in the wild in 2022 and serve as a valuable knowledge document for security teams responsible for security operations.***

Keywords: Cybersecurity**,** Zero - day, Vulnerability Management, Cyber Defense, Security Incident Response

1. Introduction

The term "Zero - Day" is derived from the fact that defenders will have no time to address the vulnerability before it is exploited. This makes these vulnerabilities valuable and lucrative for threat actors. Historically, zero - day vulnerabilities were primarily exploited by sophisticated threat actors like nation - states; now, the threat landscape has changed, and zero - days are now being extensively exploited by cybercriminals, especially ransomware groups [1] [2]. Studying zero - day vulnerabilities is important because of their unpredictable nature and the significant risks they pose to organizations. Any lessons learned from history can be useful in building future defenses. Examining these vulnerabilities can help improve defensive strategies and security tools like intrusion detection systems, endpoint protection solutions, and network security solutions. Insights gained from studying these vulnerabilities also provide valuable information about the techniques and behaviors of advanced threat actors, which can help improve threat modeling and proactive defense strategies. Identifying the most common recurring patterns in zero - day vulnerabilities will allow developers to adopt more secure coding practices, have an additional focus on the recurring themes, and address potential issues earlier in the software development lifecycle. Understanding the characteristics of zero - day vulnerabilities is essential to building a stronger and more resilient cybersecurity framework, especially as the frequency and complexity of these threats continue to evolve, and this paper aims to aid that process.

Zero - Vulnerabilities Exploited in Wild – 2022

Here is the aggregated list of zero - day vulnerabilities exploited in the wild in 2022. The table captures the CVE - ID if there is one, the vulnerable component, i. e., software, firmware, or hardware that has the vulnerability, the CWE - ID mapping (Common Weakness Enumeration), Attack Vector, and the Attack complexity. This data is sourced from publicly accessible data sources. Primarily, the data was published by NVD (National Vulnerability Database), MITRE Database, Google's threat intelligence groups, and sites like Zero - Day. Cz [2] [3] [4] The sources are chosen for quality and accuracy. These are the most publicly known zero - day vulnerabilities that were exploited in the year 2022.

Title	CVE - ID	Vulnerable Component	CWE - ID	Attack Vector	Attack Complexity
Apple iOS - Type Confusion	CVE - 2022 - 42856	Apple iOS	CWE - 843 - Type confusion	AV: N	AC: L
Citrix Access Gateway - Improper control of a resource through its lifetime	CVE - 2022 - 27518	Citrix Access Gateway	CWE - 664 - Improper control of a resource through its lifetime	AV: N	AC: L
Windows - Security features bypass	CVE - 2022 - 44698	Windows	CWE - 254 - Security Features	AV: N	AC: L
FortiOS - Heap - based buffer overflow	CVE - 2022 - 42475	FortiOS	CWE - 122 - Heap - based Buffer Overflow	AV: N	AC: L
Google Chrome - Type Confusion	CVE - 2022 - 4262	Google Chrome	CWE - 843 - Type confusion	AV: N	AC: L
Google Chrome - Heap - based buffer overflow	CVE - 2022 - 4135	Google Chrome	CWE - 122 - Heap - based Buffer Overflow	AV: N	AC: L
Windows - Security features bypass	CVE - 2022 - 41091	Windows	CWE - 254 - Security Features	AV: N	AC: L
Windows - Buffer overflow	CVE - 2022 - 41125	Windows	CWE - 119 - Memory corruption	AV: L	AC: L
Windows - Buffer overflow	CVE - 2022 - 41128	Windows	CWE - 119 - Memory corruption	AV: N	AC: L

Paper ID: SR24920135032 DOI: https://dx.doi.org/10.21275/SR24920135032

Windows - Buffer overflow	CVE - 2022 - 41073	Windows	CWE - 119 - Memory corruption	AV: L	AC: L
Apple iOS - Improper authentication	CVE - 2022 - 48618	Apple iOS	CWE - 287 - Improper Authentication	AV: L	AC: L
Google Chrome - Type Confusion	CVE - 2022 - 3723	Google Chrome	CWE - 843 - Type confusion	AV: N	AC: L
Apple iOS - Out - of - bounds write	CVE - 2022 - 42827	Apple iOS	CWE - 787 - Out - of - bounds write	AV: L	AC: L
Windows - Buffer overflow	CVE - 2022 - 41033	Windows	CWE - 119 - Memory corruption	AV: L	AC: L
bingo!CMS - Missing Authorization	CVE - 2022 - 42458	bingo!CMS	CWE - 862 - Missing Authorization	AV: N	AC: L
Microsoft Exchange Server - Server - Side Request Forgery (SSRF)	CVE - 2022 - 41040	Microsoft Exchange Server	CWE - 918 - Server - Side Request Forgery (SSRF)	AV: N	AC: L
Microsoft Exchange Server - Deserialization of Untrusted Data	CVE - 2022 - 41082	Microsoft Exchange Server	CWE - 502 - Deserialization of Untrusted Data	AV: N	AC: L
Sophos Firewall - Code Injection	CVE - 2022 - 3236	Sophos Firewall	CWE - 94 - Improper Control of Generation of Code ('Code Injection')	AV: N	AC: L
Windows - Buffer overflow	CVE - 2022 - 37969	Windows	CWE - 119 - Memory corruption	AV: L	AC: L
Apex One - Insufficient verification of data authenticity	CVE - 2022 - 40139	Apex One	CWE - 345 - Insufficient Verification of Data Authenticity	AV: N	AC: L
macOS - Buffer overflow	CVE - 2022 - 32917	macOS	CWE - 119 - Memory corruption	AV: L	AC: L
WPGateway - Improper Authorization	CVE - 2022 - 3180	WPGateway	CWE - 285 - Improper Authorization	AV: N	AC: L
BackupBuddy - Improper Authorization	CVE - 2022 - 31474	BackupBuddy	CWE - 285 - Improper Authorization	AV: N	AC: L
Photo Station - Input validation error	CVE - 2022 - 27593	Photo Station	CWE - 20 - Improper input validation	AV: N	AC: L
Google Chrome - Input validation error	CVE - 2022 - 3075	Google Chrome	CWE - 20 - Improper input validation	AV: N	AC: L
Crypto Application Server (CAS) - Improper access control	NA	Crypto Application Server (CAS)	CWE - 284 - Improper Access Control	AV: N	AC: L
macOS - Out - of - bounds write	CVE - 2022 - 32893	macOS	CWE - 787 - Out - of - bounds write	AV: L	AC: L
macOS - Out - of - bounds write	CVE - 2022 - 32894	macOS	CWE - 787 - Out - of - bounds write	AV: L	AC: L
Google Chrome - Input validation error	CVE - 2022 - 2856	Google Chrome	CWE - 20 - Improper input validation	AV: N	AC: L
Windows - Buffer overflow	CVE - 2022 - 34713	Windows	CWE - 119 - Memory corruption	AV: N	AC: L
Windows - Buffer overflow	CVE - 2022 - 22047	Windows	CWE - 119 - Memory corruption	AV: L	AC: L
Google Chrome - Heap - based buffer overflow	CVE - 2022 - 2294	Google Chrome	CWE - 122 - Heap - based Buffer Overflow	AV: N	AC: L
MiVoice Connect - OS Command Injection	CVE - 2022 - 29499	MiVoice Connect	CWE - 78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	AV: N	AC: L
Atlassian Confluence Server - Code Injection	CVE - 2022 - 26134	Atlassian Confluence Server	CWE - 94 - Improper Control of Generation of Code ('Code Injection')	AV: N	AC: L
Microsoft Word - OS Command Injection	CVE - 2022 - 30190	Microsoft Word	CWE - 78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	AV: N	AC: L
Cisco IOS XR - Improper access control	CVE - 2022 - 20821	Cisco IOS XR	CWE - 284 - Improper Access Control	AV: N	AC: L
Windows - Man - in - the - Middle (MitM) attack	CVE - 2022 - 26925	Windows	CWE - 300 - Channel Accessible by Non - Endpoint ('Man - in - the - Middle')	AV: N	AC: H
Google Chrome - Type Confusion	CVE - 2022 - 1364	Google Chrome	CWE - 843 - Type confusion	AV: N	AC: L
Windows - Buffer overflow	CVE - 2022 - 24521	Windows	CWE - 119 - Memory corruption	AV: L	AC: L

macOS - Out - of - bounds read	CVE - 2022 - 22674	macOS	CWE - 125 - Out - of - bounds read	AV: L	AC: L
macOS - Out - of - bounds write	CVE - 2022 - 22675	macOS	CWE - 787 - Out - of - bounds write	AV: L	AC: L
Apex Central - Arbitrary file upload	CVE - 2022 - 26871	Apex Central	CWE - 434 - Unrestricted Upload of File with Dangerous Type	AV: N	AC: L
Pivotal Spring Framework - Code Injection	CVE - 2022 - 22965	Pivotal Spring Framework	CWE - 94 - Improper Control of Generation of Code ('Code Injection')	AV: N	AC: L
vCenter Server - Incorrect default permissions	CVE - 2022 - 22948	vCenter Server	CWE - 276 - Incorrect Default Permissions	AV: L	AC: L
Sophos Firewall - Input validation error	CVE - 2022 - 1040	Sophos Firewall	CWE - 20 - Improper input validation	AV: N	AC: L
Google Chrome - Type Confusion	CVE - 2022 - 1096	Google Chrome	CWE - 843 - Type confusion	AV: N	AC: L
Mozilla Firefox - Use - after - free	CVE - 2022 - 26486	Mozilla Firefox	CWE - 416 - Use After Free	AV: N	AC: L
Mozilla Firefox - Use - after - free	CVE - 2022 - 26485	Mozilla Firefox	CWE - 416 - Use After Free	AV: N	AC: L
Google Chrome - Use - after - free	CVE - 2022 - 0609	Google Chrome	CWE - 416 - Use After Free	AV: N	AC: L
Adobe Commerce (formerly Magento Commerce) - OS Command Injection	CVE - 2022 - 24086	Adobe Commerce (formerly Magento Commerce)	CWE - 78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	AV: N	AC: L
Apple iOS - Use - after - free	CVE - 2022 - 22620	Apple iOS	CWE - 416 - Use After Free	AV: N	AC: L
Zimbra Collaboration - Cross - site scripting	CVE - 2022 - 24682	Zimbra Collaboration	CWE - 79 - Improper Neutralization of Input During Web Page Generation ('Cross - site Scripting')	AV: N	AC: L
Apple iOS - Buffer overflow	CVE - 2022 - 22587	Apple iOS	CWE - 119 - Memory corruption	AV: L	AC: L
Windows - Buffer overflow	CVE - 2022 - 21882	Windows	CWE - 119 - Memory corruption	AV: L	AC: L

Table 1 2022 Zero - day vulnerabilities exploited in the wild. [5 - 54]

Zero - Day Vulnerabilities Analysis

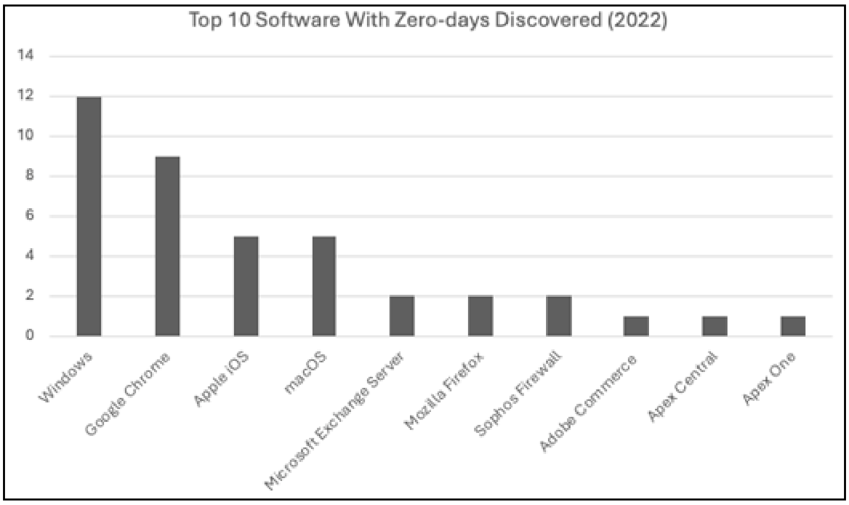

Figure 1: Top 10 software with zero - day vulnerabilities discovered in 2022 [5 - 54]

The chart depicted in Figure 1 reveals several significant patterns. Windows leads the list with the highest number of zero - day vulnerabilities, indicating that it remains a prime target for attackers. This is closely followed by Google Chrome**,** which suggests that web browsers, particularly Chrome, continue to be a critical attack surface for adversaries. Apple iOS and macOS also feature prominently, reflecting that attackers are increasingly focusing on Apple's ecosystem, likely due to its growing user base and widespread adoption in both consumer and enterprise environments. Microsoft Exchange Server appears among the top targets, emphasizing the persistent threats facing enterprise software, particularly those related to email and communication services. Additionally, other enterprise - focused software like Sophos Firewall**,** Apex Central**,** and Apex One also made the top 10, suggesting that network and security infrastructure products are also attractive targets for zero - day exploitation.

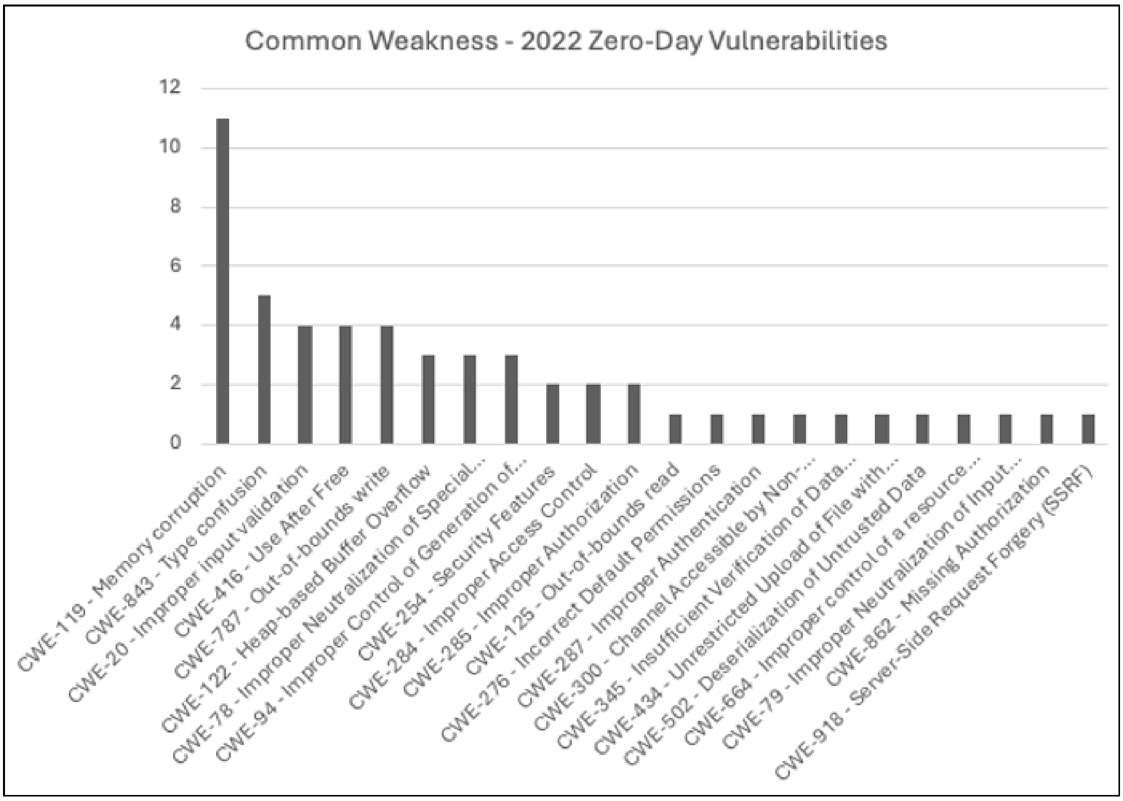

Figure 2: Common weakness enumeration mapping for 2022 zero - days [5 - 54]

Figure 2 shows the chart depicting common weaknesses exploited in zero - day vulnerabilities during 2022. It reveals significant trends that highlight the most frequent vulnerabilities targeted by attackers. Memory Corruption stands out as the most common weakness, appearing in over ten instances. Memory handling errors continue to be a critical flaw in software systems, especially in low - level programming contexts where memory management is a manual process. The next most common weakness, Improper Input Validation, is also prevalent, showing that attackers frequently exploit software that fails to adequately validate inputs, leading to conditions like buffer overflows or code injection. Other notable weaknesses are Use After Free, Integer Overflow, and Path Traversal. The chart also identifies a variety of other vulnerabilities, like Improper Authentication and Improper Access Control. We can safely conclude that most of the zero - day vulnerabilities in 2022 were the result of fundamental security weaknesses, particularly related to memory management, input validation, and access control. Again, it points to the need for software developers to focus on secure coding practices and methods to test for these weaknesses.

Table 2: Software Classification [5 - 54]

Software Name	Category
Apple iOS	End User
Citrix Access Gateway	Enterprise
Windows	Both
FortiOS	Enterprise
Google Chrome	Both
Microsoft Exchange Server	Enterprise
Sophos Firewall	Enterprise
Apex One	Enterprise
macOS	Both
WPGateway	End User
BackupBuddy	End User
Photo Station	End User
Crypto Application Server (CAS)	Enterprise
MiVoice Connect	Enterprise
Atlassian Confluence Server	Enterprise
Microsoft Word	End User
Cisco IOS XR	Enterprise
Adobe Commerce (formerly Magento)	Both
Zimbra Collaboration	Enterprise
bingo!CMS	Enterprise
Apex Central	Enterprise
Pivotal Spring Framework	Enterprise
vCenter Server	Enterprise
Mozilla Firefox	Both

Table 2 shows the classification of the software in which zero - day vulnerabilities were discovered during 2022. By categorizing the vulnerable software as end - user or enterprise, we can gain an understanding of the risk landscape and identify whether certain platforms, applications, or environments are more susceptible to zero - day attacks. This knowledge can guide the development of proactive strategies, such as enhancing monitoring or improving security measures for the most targeted platforms. Moreover, this analysis helps identify whether certain software categories like consumer - facing applications, enterprise tools, or cloud infrastructure are more prone to zero - day exploits.

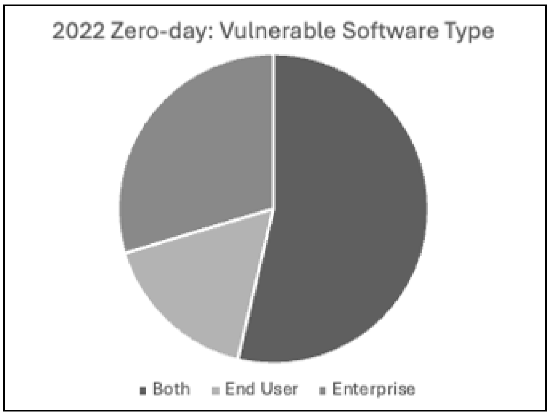

Figure 3: Vulnerable Software type distribution. [5 - 54]

The pie chart in Figure 3 shows a breakdown of the types of software in which zero - day vulnerabilities were discovered. From the chart, we can observe that Enterprise software constitutes the largest portion of vulnerabilities, reflecting its significant exposure and attractiveness to attackers. Given the critical nature of enterprise environments, where sensitive data and mission - critical operations are often handled, it is not surprising that attackers focus heavily on exploiting these systems. The category “Both” represents software used in both personal and business contexts, such as web browsers, operating systems, and other cross - platform tools. This further adds weight to the enterprise category. We can safely conclude that in 2022, large portions of the zero - day exploits were against enterprise software. This correlates very well with the rise of ransomware groups.

Key Insights for Defenders

The analysis showed an increased targeting of enterprise software, and the recurring theme of memory management issues, misconfigurations, poor coding practices, and weak authentication and authorization are the top weaknesses resulting in these zero days. Though not surprising, it is vital to look at history and plan for the future with the lessons learned. Organizations should continue to focus on fundamental security best practices to prevent such weaknesses from appearing in the software.

There is no silver bullet to prevent zero - days; an overall security posture improvement, mature IT asset inventory, and a high degree of visibility into what applications, application dependencies, installed software, and continuous compliance monitoring for security policies and security best practices will put the organization into a better position to respond to zero - day vulnerability situations.

2. Conclusion

By analyzing zero - day vulnerabilities in 2022, the paper aimed to present insights to help organizations devise strategies. The analysis showed that the most targeted systems, including Windows, Google Chrome, and enterprise software such as Microsoft Exchange Server and Sophos Firewall, demonstrate that attackers continue to exploit widespread platforms with high impact potential. Some of the notable weaknesses, like memory corruption issues, improper input validation, and weak authentication mechanisms, emerged as common vulnerabilities, reiterating the fundamental challenges in secure software development. The breakdown of vulnerabilities by software type showed a clear inclination toward enterprise software, indicating that attackers are increasingly focused on exploiting systems that manage sensitive data and critical operations. This aligns with the rise of ransomware and other financially motivated attacks targeting enterprises. While 2022 saw a reduction in the number of zero - day vulnerabilities compared to previous years, the threat remains significant. Organizations must prioritize secure coding practices and proactive measures like continuous compliance monitoring, a mature IT asset inventory, and strong security policies, which are vital for improving an organization's ability to detect, respond to, and recover from zero - day vulnerabilities.

References

[1] Google. (2022). Zero - days exploited in 2022. Google Cloud Blog. https: //cloud. google. com/blog/topics/threat - intelligence/zero - days - exploited - 2022

[2] MITRE. CVE. https: //cve. mitre. org/

[3] National Institute of Standards and Technology. (n. d.). National Vulnerability Database (NVD). https: //nvd. nist. gov/

[4] Zero - Day CZ. Zero - day vulnerabilities. https: //www.zero - day. cz/

[5] Apple. (2022). About the security content of macOS Monterey 12.6.2. https: //support. apple. com/en - us/HT213516

[6] Citrix. (2022, December 13). Critical security update now available for Citrix ADC and Citrix Gateway. https: //www.citrix. com/blogs/2022/12/13/critical - security - update - now - available - for - citrix - adc - citrix - gateway/

[7] Microsoft. (2022). CVE - 2022 - 44698. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 44698

[8] Fortinet. (2022). FortiGuard PSIRT advisory FG - IR - 22 - 398. https: //fortiguard. fortinet. com/psirt/FG - IR - 22 - 398

[9] Google. (2022, December). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/12/stable - channel - update - for - desktop. html

[10] Google. (2022, November 24). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/11/stable - channel - update - for - desktop_24. html

[11] Microsoft. (2022). CVE - 2022 - 41091. Microsoft Security Update Guide. https: //portal. msrc. microsoft. com/en - US/security - guidance/advisory/CVE - 2022 - 41091

[12] Microsoft. (2022). CVE - 2022 - 41125. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 41125

[13] Microsoft. (2022). CVE - 2022 - 41073. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 41073

[14] Apple. (2022). About the security content of iOS 16.2 and iPadOS 16.2. https: //support. apple. com/en - us/HT213530

[15] Google. (2022, October 27). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/10/stable - channel - update - for - desktop_27. html

[16] Apple. (2022). About the security content of macOS Ventura 13.0.1. https: //support. apple. com/en - us/HT213489

[17] Microsoft. (2022). CVE - 2022 - 41033. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 41033

[18] Microsoft. (2022, September 29). Customer guidance for reported zero - day vulnerabilities in Microsoft Exchange Server. https: //msrc - blog. microsoft. com/2022/09/29/customer - guidance - for - reported - zero - day - vulnerabilities - in - microsoft - exchange - server/

[19] GTEL TSC. (2022). Warning: New attack campaign utilized a new 0day RCE vulnerability on Microsoft Exchange Server. https: //gteltsc. vn/blog/warning - new - attack - campaign - utilized - a - new - 0day - rce - vulnerability - on - microsoft - exchange - server - 12715. html

[20] Sophos. (2022, September 23). Sophos SA - 20220923 SFOS RCE. https: //www.sophos. com/en - us/security - advisories/sophos - sa - 20220923 - sfos - rce

[21] Microsoft. (2022). CVE - 2022 - 37969. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 37969

[22] Trend Micro. (2022). Threat analysis report for RCE exploit in CVE - 2022 - 22963. https: //success. trendmicro. com/jp/solution/000291471

[23] Apple. (2022). About the security content of iOS 16.1. https: //support. apple. com/en - us/HT213444

[24] Wordfence. (2022, September). PSA: Zero - day vulnerability in WP Gateway actively exploited in the wild. https: //www.wordfence. com/blog/2022/09/psa - zero - day - vulnerability - in - wpgateway - actively - exploited - in - the - wild/

[25] iThemes. (2022, September 6). WordPress vulnerability report special edition: BackupBuddy. https: //ithemes. com/blog/wordpress - vulnerability - report - special - edition - september - 6 - 2022 - backupbuddy/

[26] QNAP. (2022). QNAP Security Advisory QSA - 22 - 24. https: //www.qnap. com/en/security - advisory/qsa - 22 - 24

[27] Google. (2022, September). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/09/stable - channel - update - for - desktop. html

[28] General Bytes. (2022, August 18). Security incident August 18th 2022. https: //generalbytes. atlassian. net/wiki/spaces/ESD/pages/2785509377/Security+Incident+August+18th+2022

[29] Apple. (2022). About the security content of iOS 16. https: //support. apple. com/en - us/HT213412

[30] Apple. (2022). About the security content of iOS 16. https: //support. apple. com/en - us/HT213412

[31] Google. (2022, August 16). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/08/stable - channel - update - for - desktop_16. html

[32] Microsoft. (2022). CVE - 2022 - 34713. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 34713

[33] Microsoft. (2022). CVE - 2022 - 22047. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 22047

[34] Google. (2022, July). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/07/stable - channel - update - for - desktop. html

[35] Mitel. (2022). Mitel Product Security Advisory 22 - 0002. https: //www.mitel. com/support/security - advisories/mitel - product - security - advisory - 22 - 0002

[36] Nao_sec. (2022, May 27). Twitter post. https: //twitter. com/nao_sec/status/1530196847679401984

[37] Cisco. (2022). Cisco IOS XR Redis Security Advisory. https: //tools. cisco. com/security/center/content/CiscoSecurityAdvisory/cisco - sa - iosxr - redis - ABJyE5xK

[38] Microsoft. (2022). CVE - 2022 - 26925. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 26925

[39] Google. (2022, April 14). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/04/stable - channel - update - for - desktop_14. html

[40] Microsoft. (2022). CVE - 2022 - 24521. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 24521

[41] Apple. (2022). About the security content of macOS Monterey 12.3. https: //support. apple. com/en - us/HT213220

[42] Apple. (2022). About the security content of macOS Monterey 12.3. https: //support. apple. com/en - us/HT213220

[43] Trend Micro. (2022). Trend Micro update on Spring4Shell. https: //success. trendmicro. com/dcx/s/solution/000290678?language=en_US

[44] Wallarm. (2022). Update on 0 - day vulnerabilities in Spring4Shell and CVE - 2022 - 22963. https: //lab. wallarm. com/update - on - 0 - day - vulnerabilities - in - spring - spring4shell - and - cve - 2022 - 22963/

[45] Sophos. (2022, March 25). Sophos SA - 20220325 SFOS RCE. https: //www.sophos. com/en - us/security - advisories/sophos - sa - 20220325 - sfos - rce

[46] Google. (2022, March 25). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/03/stable - channel - update - for - desktop_25. html

[47] Mozilla. (2022). MFSA 2022 - 09 security advisory. https: //www.mozilla. org/en - US/security/advisories/mfsa2022 - 09/

[48] Mozilla. (2022). MFSA 2022 - 09 security advisory. https: //www.mozilla. org/en - US/security/advisories/mfsa2022 - 09/

[49] Google. (2022, February 14). Stable channel update for desktop. Chrome Releases. https: //chromereleases. googleblog. com/2022/02/stable - channel - update - for - desktop_14. html

[50] Adobe. (2022). Magento APSB22 - 12 security bulletin. https: //helpx. adobe. com/security/products/magento/apsb22 - 12. html

[51] Apple. (2022). About the security content of macOS Monterey 12.2.1. https: //support. apple. com/en - us/HT213093

[52] Volexity. (2022, February 3). Operation EmailThief: Active exploitation of zero - day XSS vulnerability in Zimbra. https: //www.volexity. com/blog/2022/02/03/operation - emailthief - active - exploitation - of - zero - day - xss - vulnerability - in - zimbra/

[53] Apple. (2022). About the security content of macOS Monterey 12.2. https: //support. apple. com/en - us/HT213053

[54] Microsoft. (2022). CVE - 2022 - 21882. Microsoft Security Update Guide. https: //msrc. microsoft. com/update - guide/en - US/vulnerability/CVE - 2022 - 21882