International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I9P128

Volume 72 Issue 9, 176-184, September 2024

Original Article

Digital Ground Zero: An In-Depth Analysis of 2023's Zero-Day Vulnerabilities

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA.

Corresponding Author : varadharaj.krishnan@gmail.com

Received: 12 August 2024 Revised: 09 September 2024 Accepted: 26 September 2024 Published: 30 September 2024

Abstract *- A distinct challenge is posed by zero-day vulnerabilities to security teams within an organization. These types of vulnerabilities enable attackers to exploit software flaws before patches are available. In 2023, the number and complexity of Zero-Day exploits increased substantially. Nation-state actors, cybercriminal groups, and commercial surveillance vendors are taking advantage of these vulnerabilities more than ever. This paper provides a comprehensive analysis of the Zero-Day vulnerabilities discovered and exploited in 2023. Based on public data sources like Google's Threat Analysis Group (TAG), MITRE's CVE database, and Zero-Day.cz, this study examines trends, attack vectors, and the most targeted software platforms. Through empirical analysis, trends and patterns are discovered to devise strategies to defend against them or mitigate them. The paper explores key defense strategies like Zero Trust Architecture, real-time threat intelligence integration, and mature Endpoint Detection and Response (EDR) solutions to prevent, detect, and respond to exploits using the zero-day vulnerability. By understanding the history of incidents and vulnerability disclosures, this paper aims to provide actionable insights for organizations looking to strengthen their cybersecurity defenses and prepare for future Zero-Day exploits.*

Keywords *- Zero-day vulnerability, Zero-day, Cyber defense, Security operations, Incident response.*

1. Introduction

According to the NIST (National Institute of Standards and Technology), a zero-day vulnerability is a previously unknown flaw in software or hardware that hackers can exploit to attack systems. The term "zero-day" refers to the fact that the vendor has had "zero days" to address the issue. These vulnerabilities are significant in the cybersecurity space because they represent a race against time, where Attackers aim to exploit these vulnerabilities before the software or hardware vendor becomes aware of them and patches them. Defenders scramble to identify and mitigate the threat. Zero-day vulnerabilities are prized by attackers because there is no known fix for them and the possibility of a high success rate when using them. Also, it provides a direct bypass to the target despite various layers of security controls that might be in place. From a national security standpoint, Zero-Day vulnerabilities have become a key pathway for state-sponsored cyber espionage. Governments often use them to gain unauthorized access to the systems of their adversaries. In recent years, the rise of ransomware and other financially motivated cybercrime groups has further made these vulnerabilities highly prized. In the year 2023, cybersecurity experts observed a good increase in the number of exploits using zero-day vulnerabilities. According to Google's Threat Analysis Group (TAG) and Mandiant, approximately 97 Zero-Day vulnerabilities were exploited in the wild in 2023, a 50% increase from 2022 [1]. The objective of this paper is to provide a comprehensive analysis of the Zero-Day vulnerabilities discovered and exploited in 2023. By analyzing these vulnerabilities, trends, and the characteristics of the attack, this paper aims to provide insights for organizations to strengthen their defenses and develop strategies to improve their defense against attacks that use Zero-Day vulnerabilities.

2. Background

Zero-day vulnerabilities have a long history in the cybersecurity world. As stated earlier, the concept of a "Zero-Day" stems from the fact that the defenders have zero days to address and patch a vulnerability before it is exploited. This makes them valuable, dangerous, and lucrative for threat actors. Historically, Zero-Day vulnerabilities were primarily used by sophisticated attackers like nation-states. For example, Stuxnet from the year 2010 showed the world the devastating potential of such vulnerabilities [2]. It was a state-sponsored attack targeting Iran's nuclear program; the attack leveraged multiple Zero-Day vulnerabilities to disable industrial control systems controlling the plant [3]. Since then, the threat landscape has changed gradually to a situation where Zero-Day exploits were once primarily used for espionage and military purposes and have now been

increasingly used by cybercriminals, especially Ransomware gangs. Groups like FIN11 and REvil have demonstrated how Zero-Day vulnerabilities can be weaponized for financial gain [5][6]. In parallel, the rise of the dark web and underground markets have created a thriving economy for trading exploits using Zero-Day vulnerabilities. Today, some Zero-Day exploits fetch up to $1 million, depending on their target. Lastly, the emergence of Commercial Surveillance Vendors (CSVs), who sell spyware and hacking tools to governments, further fueled the discovery and exploitation of Zero-Day vulnerabilities [5][6].

The Zero-Day vulnerabilities are discovered through several channels. On the legitimate side, organizations offer "Bug Bounty" programs where ethical hackers are rewarded for discovering and reporting vulnerabilities before they can be exploited. Organizations like Google, Apple, and Microsoft have invested heavily in such programs to reduce the risk posed by undiscovered flaws. Bug bounties were introduced to create an incentive model for hackers to be on the legitimate side; it incentivizes researchers to report vulnerabilities rather than sell them to malicious actors. On the other hand, cybercriminal organizations and nation-state actors actively trade the knowledge of the vulnerability and exploits that have not been disclosed to vendors.

Spyware vendors providing service to governments and law enforcement agencies are often at the center of these trades. These vendors purchase vulnerabilities and use them to build sophisticated exploit kits to sell them to their clients. According to a Google report, In 2023, CSVs were responsible for nearly 50% of all known Zero-Day vulnerabilities [6].

3. Methodology

This study primarily used data from publicly available sources. First, data from reliable, publicly accessible sources like Google's Threat Analysis Group (TAG), MITRE's CVE (Common Vulnerabilities and Exposures) database, the NVD (National Vulnerability Database), and data from Zero-Day.cz were used [1-4]. Additionally, industry-specific blogs and cybersecurity news outlets like Bleeping Computer and SecurityWeek and reports from independent researchers were used to validate the vulnerabilities reported by larger entities. After collecting the data, a systematic analysis was conducted to break down the vulnerabilities into several dimensions. This study explored Attack Vectors, Targeted Platforms, Exploiting Actors, Vulnerable Components and Types, and various attributes defined by CVSS scoring methodology.

4. Zero-Day Vulnerabilities Analysis

When plotting the top 10 vulnerable software components affected by zero-day vulnerabilities in 2023, Apple iOS and Windows stand out as the top two platforms with the highest number of vulnerabilities in 2023, with approximately 18 and 16 Zero-Day vulnerabilities discovered, respectively. It also means that attackers are heavily targeting widely used platforms. The popularity of Windows in enterprise environments and iOS's dominance in mobile devices made them lucrative targets.

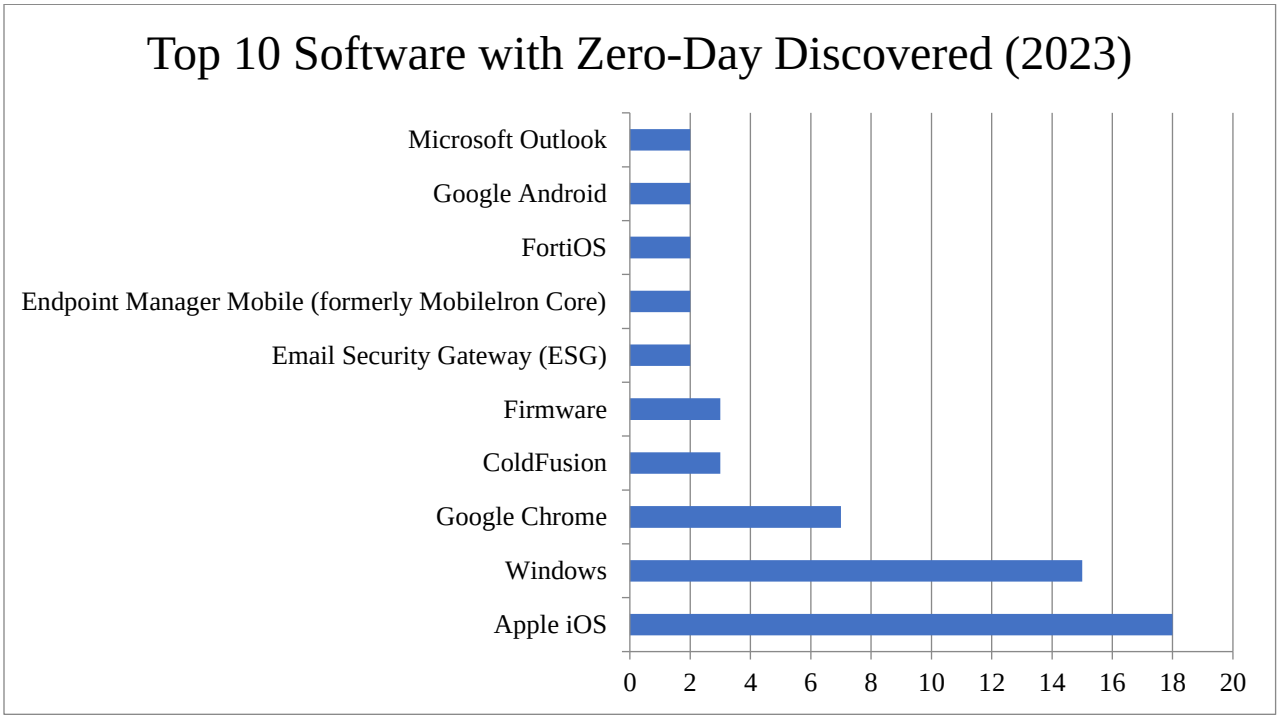

Fig. 1 Top 10 software with zero-day discovered in 2023 [12-84]

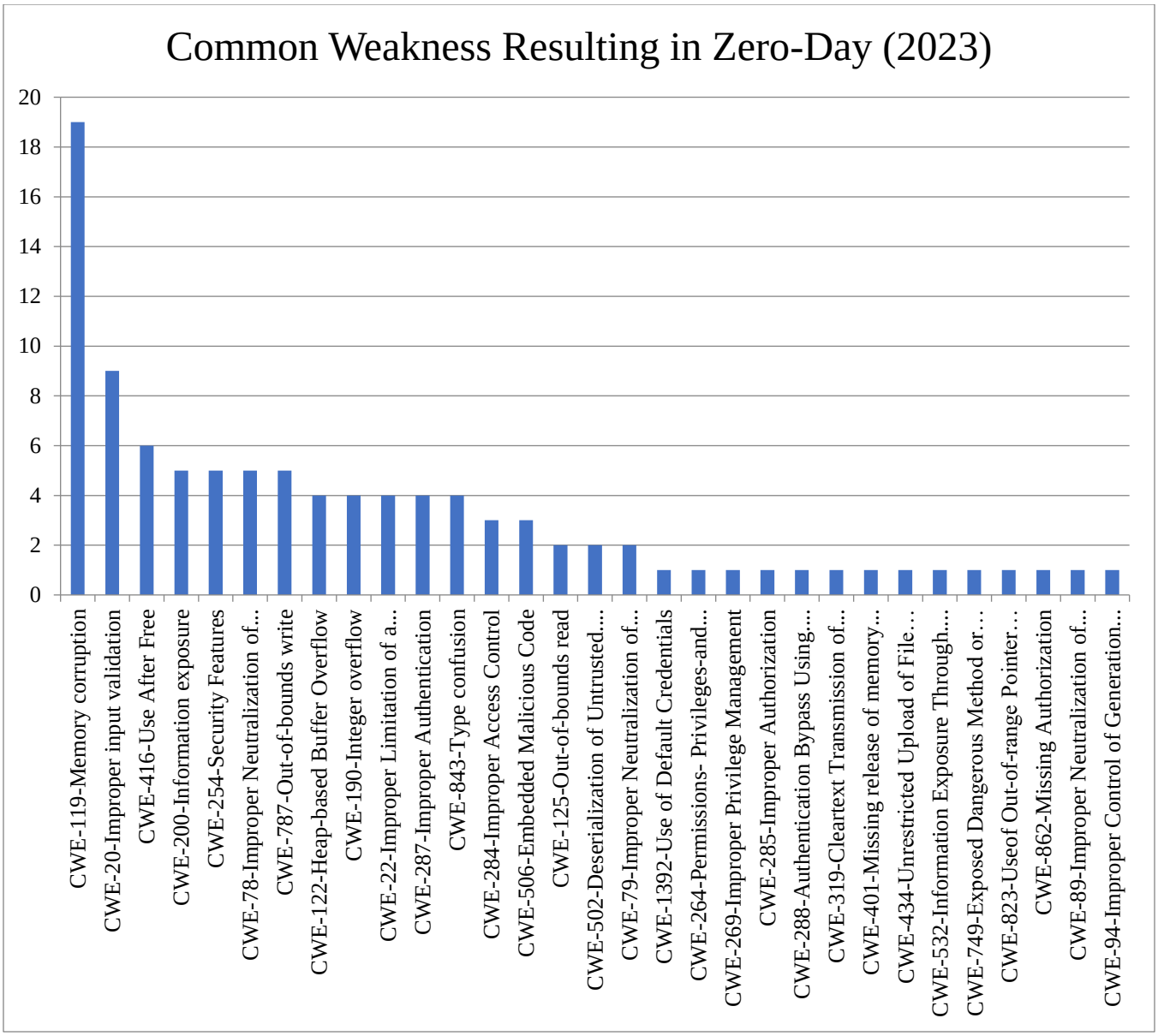

Fig. 2 Common weakness results in zero-day in 2023 [12-87]

Fig. 3 2023 Zero-day vulnerability distribution [12-87]

Google Chrome, too, has a notable number of Zero-Day vulnerabilities. Chrome is the most widely used web browser globally, and attackers are naturally motivated to find vulnerabilities in it. Enterprise products like FortiOS, Endpoint Manager Mobile, and Email Security Gateway (ESG) are also being increasingly targeted. Cybercriminal groups, especially ransomware gangs, are financially motivated to target enterprises. Overall, the most significant Zero-Day vulnerabilities were found in platforms used by millions of individuals and enterprises worldwide. This indicates that the attackers prioritize high-impact platforms for their exploits. The focus on desktop (Windows, iOS) and mobile platforms (Android, iOS) shows a broad scope of attack vectors aimed at compromising personal and corporate environments. Lastly, security software and infrastructure products being on the list show a growing trend where attackers focus on breaching critical defenses that could lead to greater access and control over networks and sensitive data.

When plotting the CWE (Common Weakness and Exposure) that led to the vulnerability. Memory Corruption is the most frequent common weakness, leading to Zero-Day vulnerabilities in 2023, with close to 20 occurrences. This is a well-known weakness that attackers exploit to execute arbitrary code or cause system crashes. Memory corruption remains one of the most dangerous vulnerabilities because it allows attackers to manipulate memory and gain unauthorized access to sensitive areas of the system, potentially leading to privilege escalation or complete system compromise. Another significant common weakness was Improper Input Validation, and the use of After Free also appeared frequently. Improper Input Validation occurs when software fails to validate inputs properly, allowing attackers to inject malicious input, potentially leading to injection attacks or buffer overflows. Use After Free happens when a program continues to use memory after it has been freed, which attackers can exploit to execute arbitrary code. This weakness is common in software that manages dynamic memory. Many vulnerabilities fall under improper memory handling or input validation issues (e.g., memory corruption, use-after-free, buffer overflows). This suggests attackers continue exploiting fundamental weaknesses in how software manages memory and processes input. Developers should prioritize strengthening these areas (memory safety and input validation) to reduce Zero-Day vulnerabilities.

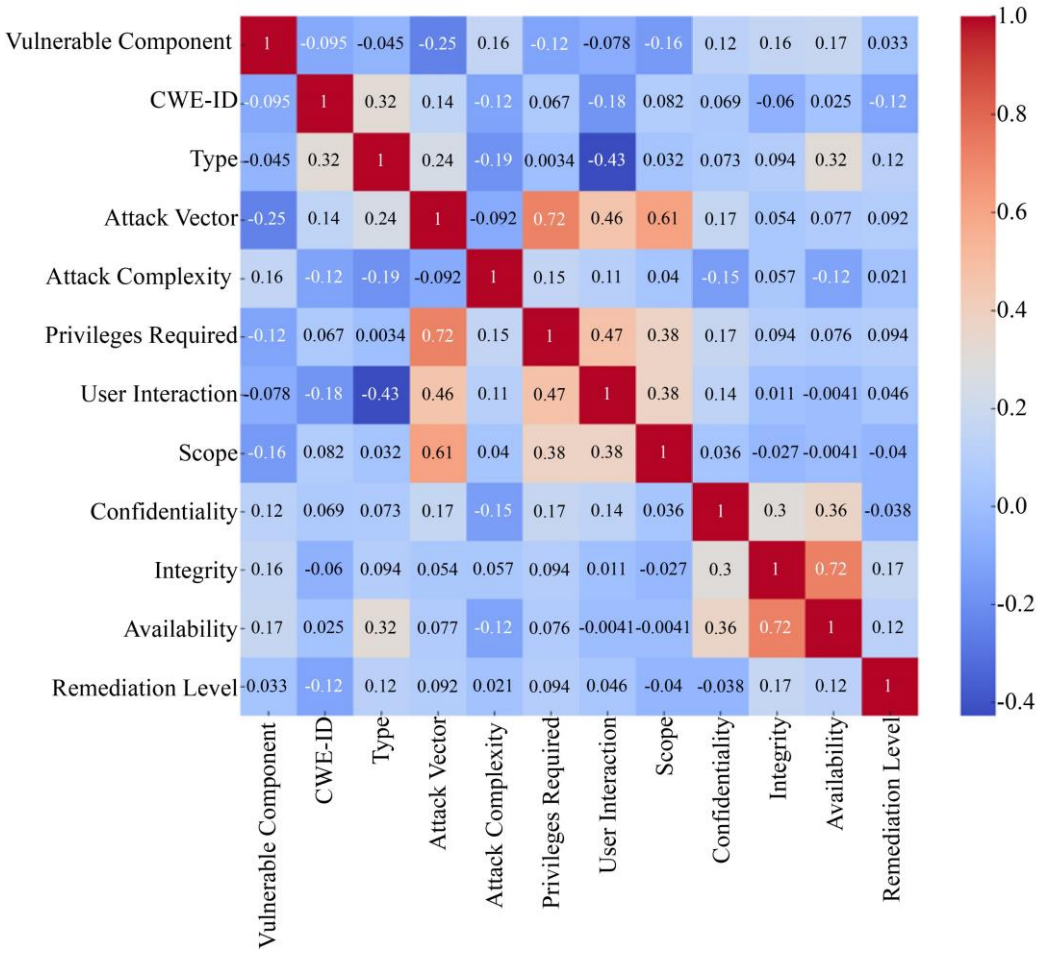

Fig. 4 2023 Zero-day vulnerability attributes correlation heatmap. [12-82]

The majority of Zero-Day vulnerabilities in 2023 impacted End Users and platforms that both end users and enterprises use. End User software accounts for a significant portion of the vulnerabilities, indicating that attackers continue to focus heavily on widely used consumer platforms (like operating systems, browsers, and mobile apps) that have a broad user base. Enterprise-only software accounts for a smaller portion. Network-based attacks are the dominant attack vector for Zero-Day vulnerabilities in 2023; it shows how attackers exploit vulnerabilities over the internet or organizational networks. Local attacks, which require physical or local access to the system, form a smaller portion of the vulnerabilities. However, they remain relevant for attacks on specific high-value targets or where local compromise can lead to lateral movement within a network. Lastly, a significant portion of vulnerabilities require no user interaction, meaning that attackers can exploit these vulnerabilities without needing the user to take any action, such as clicking a malicious link or opening a file. Vulnerabilities where User Interaction is Required still account for a notable portion. These types of attacks often rely on phishing or social engineering to trick users into enabling the exploit. Though more manual in nature, they remain a potent attack vector for hackers, especially in targeted attacks.

There is a significant positive correlation (0.72) between Attack Vector and the Privileges Required. It indicates that some attack vectors need elevated privileges for successful exploitation. For example, attackers using vectors like remote code execution would require admin or root access. A moderate positive correlation (0.46) between User Interaction and Attack Vector suggests that certain methods, such as phishing or social engineering, often involve end users. Therefore, attackers might depend on user actions to exploit vulnerabilities. A moderate correlation (0.38) between Privileges Required and Scope indicates that as required privileges increase, the impact's scope broadens. Vulnerabilities needing higher privileges typically affect larger system or network areas.

The strong correlation of 0.72 between Integrity and Availability, as well as the moderate correlation of 0.36 between Confidentiality and both Integrity and Availability, suggest that when a vulnerability affects one element of the CIA triad, it often impacts the others as well. This implies that Zero-Day vulnerabilities often compromise multiple security dimensions simultaneously. A mild positive correlation (0.16) between Attack Complexity and Vulnerable Components indicates that some vulnerable components are linked to more complex exploits. This may suggest the advanced techniques needed to target specific systems or software. There is a moderate positive correlation (0.32) between Type and CWE-ID, indicating that certain vulnerability types (such as enterprise-specific or others) are more likely associated with specific weaknesses as defined by the CWE system. A slight positive correlation (0.15) between Privileges Required and Attack Complexity indicates that more intricate attacks might need higher privileges, although this relationship is weak.

5. Defense Strategies and Mitigation

Exploiting a Zero-Day vulnerability typically follows a pattern. First, the attacker identifies or purchases the knowledge about the vulnerability and builds a method for exploiting it. Most often, the exploit will be in the form of a malware payload or exploit chain. The attacker then leverages this exploit to gain unauthorized access to a target system. Since the vulnerability is unknown, traditional security defenses like firewalls and intrusion detection systems are often ineffective, allowing the attacker to move laterally through the network undetected.

Privilege escalation techniques are commonly used to gain full control over the compromised system. Once the exploit is successful, attackers can carry out a variety of malicious actions, from exfiltrating sensitive data to deploying ransomware. In 2023, ransomware groups like FIN11 exploited Zero-Day vulnerabilities in enterprise software to streamline attacks and increase their ransom demands [4][5].

As the volume and complexity of Zero-Day vulnerabilities continue to rise, defense strategies should evolve. Though there is no silver bullet to address this issue, an overall security posture improvement, and mature IT asset inventory are. A high degree of visibility into what applications, application dependencies, installed software, and continuous compliance monitoring for security policies and security best practices can prevent some. It will also put the organization in a better position to respond to zero-day vulnerability situations. In addition to this, the adoption of various technical capabilities can further strengthen the overall security posture in the context of zero-day vulnerabilities [6][7].

5.1. Zero Trust Architecture

One of the most robust defense strategies in response to Zero-Day vulnerabilities is adopting a Zero Trust Network Access Architecture (ZTNA). Zero Trust shifts the security paradigm by assuming that no part of the network is inherently trustworthy, whether internal or external. This approach continuously validates access requests and ensures that users and devices have the least amount of privilege necessary to perform their functions.

In a zero-trust environment, segmentation and strict access control measures are applied across the network. Even if a Zero-Day exploit grants an attacker access to one system, lateral movement will be minimized, reducing the overall impact of the breach.

5.2. Threat Intelligence and Vulnerability Scanning

A mature threat intelligence program will help organizations stay updated on emerging Zero-Day vulnerabilities and attack trends associated with them. By integrating real-time threat intelligence feed into their security systems, organizations can detect potential indicators of Zero-Day vulnerabilities and possible indicators of compromise. Vulnerability scanning tools, although unable to detect a Zero-Day directly, should be used to identify known vulnerabilities, and they should be remediated. Doing so will reduce the opportunity for the attacker to move laterally. Secondly, regular vulnerability assessments can help security teams prioritize patch efforts and identify configurations that could be leveraged by unknown vulnerabilities [8].

5.3. Patch Management and Advanced Traffic Management Capabilities

While Zero-Day vulnerabilities exploit unpatched software, having a robust patch management strategy is vital to shrink the window of exposure once a patch becomes available. Organizations should strive to reduce the time between a vendor's release of a patch and the actual deployment of the patch across the organization. In cases where patching is not possible, organizations should have web application firewalls and network firewalls to block attack vectors associated with the vulnerability, buying time until an official patch can be applied [9][10][11].

5.4. Endpoint Detection and Response (EDR)

EDR solutions provide continuous monitoring and visibility across endpoints, such as laptops, servers, and mobile devices. EDR tools are equipped with behavioral analytics and machine learning capabilities to detect abnormal behavior such as privilege escalation, lateral movement, or the execution of unauthorized code. By correlating suspicious activities across endpoints, EDR systems can flag the potential second stage of the attack or lateral movement. EDR agents can automatically respond by quarantining suspicious files. A more sophisticated deployment of extended detection and response (XDR) with integration into other products deployed to defend at various layers of the network and application can enhance the detection of Zero-Day attacks by correlating indicators from other sources.

5.5. Incident Response and Crisis Management

A mature incident response plan is critical to limiting the impact of a Zero-Day attack once detected [9][11]. Organizations must prepare to identify and isolate affected systems quickly, understand the scope of the breach, and implement containment measures. Incident response teams should have pre-established protocols for responding to Zero-Day vulnerabilities, including collaboration with external vendors and security researchers for patches and forensic investigation. Regular crisis management drills that simulate Zero-Day attacks can also ensure that both technical teams and executive management are prepared to respond effectively in a real-world scenario.

6. Conclusion

Zero-day vulnerabilities create a distinct challenge for security teams. This study identified trends and derived insights from Zero-Day vulnerabilities from 2023, which can be used for organizations to strengthen their security posture better and improve security operations processes. Prominent platforms, including Windows, Apple iOS, and Google Chrome, were primary targets, indicating that attackers persist in prioritizing high-impact, extensively utilized systems for their exploits. The study also found that network-based attacks constitute the primary attack vector. Organizations must employ a blend of preventative and reactionary tactics to mitigate Zero-Day threats. Zero Trust Architecture, real-time threat intelligence, and Endpoint Detection and Response (EDR) solutions are essential elements of a holistic protection approach. Organizations can further mitigate risks by consistently monitoring for anomalous behavior, restricting lateral movement, and prompt patching of vulnerabilities. Although Zero-Day vulnerabilities are inherently unpredictable, implementing a multi-layered security strategy and prioritizing fast-reaction capabilities can substantially mitigate the chance of exploitation. The conclusions and methodologies presented in this research offer significant insights for organizations aiming to strengthen their defense posture.

References

[1] Maddie Stone, and James Sadowski, A Review of Zero-day in-the-wild Exploits in 2023, Google The Keyword, 2024. [Online]. Available: https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/

[2] We're All in this Together, A Year in Review of Zero-Days Exploited in-the-wild in 2023, Google, 2024. [Online]. Available: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

[3] Buying Spying: Insights into Commercial Surveillance Vendors, Google. [Online]. Available: https://storage.googleapis.com/gweb-uniblog-publiksh-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors.pdf

[4] Zero-day Vulnerability Database, Zero-Day.cz. [Online]. Available: https://www.zero-day.cz/database/?set_filter=Y&arrFilter_pf%5BYEAR_FROM%5D=2023&arrFilter_pf%5BYEAR_TO%5D=2023&arrFilter_pf%5BSEARCH%5D=

[5] Sergiu Gatlan, Google: Spyware Vendors Behind 50 Percent of Zero-days Exploited in 2023, BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/google-spyware-vendors-behind-50-percent-of-zero-days-exploited-in-2023/
[6] Jonathan Greig, Zero-day Exploited in the Wild Jumped in 50% in 2023, Fueled by Spyware Vendors, The Record, 2024. [Online]. Available: https://therecord.media/zero-day-exploits-jumped-in-2023-spyware
[7] Mandiant, Google Cloud, Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft, 2023. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft
[8] Venkatesh Sundararajan, Zero-day Vulnerability – Examples, Detection & Prevention [+ Monthly 0-day Reports], Indusface, 2024. [Online]. Available: https://www.indusface.com/blog/zero-day-vulnerability/
[9] Tenable, Understanding Zero-Day Vulnerabilities, Exploits and Attacks. [Online]. Available: https://www.tenable.com/source/zero-day
[10] Kapil Raina, What is a Zero-Day Exploit?, CrowdStrike, 2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/
[11] IBM, What is a Zero-Day Exploit?. [Online]. Available: https://www.ibm.com/topics/zero-day
[12] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html
[13] Ledger, [Twitter post]. X (Formerly Twitter), 2023. [Online]. Available: https://twitter.com/Ledger/status/1735291427100455293
[14] Apple, About the Security Content of iOS 16.7. [Online]. Available: https://support.apple.com/en-us/HT214033
[15] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html
[16] Cybersecurity and Infrastructure Security Agency (CISA), Exploitation of Unitronics PLCs used in Water and Wastewater Systems, 2023. [Online]. Available: https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems
[17] Microsoft, CVE-2023-36033: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36033
[18] Microsoft, CVE-2023-36025: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025
[19] Microsoft, CVE-2023-36036: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36036
[20] SysAid, SysAid On-premise Software CVE-2023-47246 Vulnerability, 2023. [Online]. Available: https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification
[21] Cisco, Multiple Vulnerability in Cisco IOS XE web UI Feature, 2023. [Online]. Available: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
[22] Wordfence, PSA: Critical Unauthenticated Arbitrary File Upload Vulnerability in Royal Elementor Addons and Templates being Actively Exploited, 2023. [Online]. Available: https://www.wordfence.com/blog/2023/10/psa-critical-unauthenticated-arbitrary-file-upload-vulnerability-in-royal-elementor-addons-and-templates-being-actively-exploited/
[23] Microsoft, CVE-2023-36563: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36563
[24] Microsoft, CVE-2023-41763: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-41763
[25] Jira, Broken Authentication & Session Management in Confluence Data Center and Server - CVE-2023-22515. [Online]. Available: https://jira.atlassian.com/browse/CONFSERVER-92475
[26] Apple, About the Security Content of iOS 16.5. [Online]. Available: https://support.apple.com/en-us/HT213961
[27] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html
[28] Cisco, Cisco IOS and IOS XE Software Cisco Group Encrypted Transport VPN Software Out-of-Bounds Write Vulnerability. [Online]. Available: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx
[29] Apple, About the Security Content of iOS 16.4.1. [Online]. Available: https://support.apple.com/en-us/HT213927
[30] Trend Micro, CRITICAL SECURITY BULLETIN: 3rd Party AV Uninstaller Module for Trend Micro Apex One and Worry-Free Business Security Arbitrary Code Execution Vulnerability. [Online]. Available: https://success.trendmicro.com/dcx/s/solution/000294994?language=en_US
[31] Source, Pixel Update Bulletin—September 2023. [Online]. Available: https://source.android.com/docs/security/bulletin/pixel/2023-09-01
[32] Microsoft, CVE-2023-36802: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36802

[33] Microsoft, CVE-2023-36761: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36761
[34] Adobe, Security Updates Available for Adobe Acrobat and Reader | APSB23-34. [Online]. Available: https://helpx.adobe.com/security/products/acrobat/apsb23-34.html
[35] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
[36] Apple, About the Security Content of iOS 16.2. [Online]. Available: https://support.apple.com/en-us/HT213905
[37] Google, Android Security Bulletin: September 2023. [Online]. Available: https://source.android.com/docs/security/bulletin/2023-09-01
[38] Ivanti, CVE-2023-38035: API Authentication Bypass on Sentry Administrator Interface, 2023. [Online]. Available: https://forums.ivanti.com/s/article/CVE-2023-38035-API-Authentication-Bypass-on-Sentry-Administrator-Interface?language=en_US
[39] Safe-Surf, Specialists' News. [Online]. Available: https://safe-surf.ru/specialists/news/697426/
[40] Microsoft, CVE-2023-38180: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-38180
[41] Avast, Guptiminer: Hijacking Antivirus Updates for Distributing Backdoors and Casual Mining, 2024. [Online]. Available: https://decoded.avast.io/janrubin/guptiminer-hijacking-antivirus-updates-for-distributing-backdoors-and-casual-mining/
[42] Ivanti, CVE-2023-35081 – Remote Arbitrary File Write, 2023. [Online]. Available: https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US
[43] BleepingComputer, Ivanti Patches MobileIron Zero-day Bug Exploited in Attacks, 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/ivanti-patches-mobileiron-zero-day-bug-exploited-in-attacks/
[44] Apple, About the Security Content of iOS 16.3. [Online]. Available: https://support.apple.com/en-us/HT213842
[45] Adobe, Security Updates available for Adobe ColdFusion | APSB23-47, 2023. [Online]. Available: https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html
[46] Citrix, Citrix ADC and Citrix Gateway security bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467, 2023. [Online]. Available: https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467
[47] BleepingComputer, Rockwell Warns of New APT RCE Exploit Targeting Critical Infrastructure, 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/rockwell-warns-of-new-apt-rce-exploit-targeting-critical-infrastructure/
[48] Microsoft, Storm-0978 Attacks Reveal Financial and Espionage Motives. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/
[49] Microsoft, CVE-2023-35311: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-35311
[50] Microsoft, CVE-2023-36874: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36874
[51] Microsoft, CVE-2023-32049: Security Advisory, 2023. [Online] Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-32049
[52] Microsoft, CVE-2023-32046: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-32046
[53] WordPress, Security Issue. [Online]. Available: https://wordpress.org/support/topic/security-issue-144/#post-16859857
[54] Apple, About the Security Content of iOS 16.1. [Online]. Available: https://support.apple.com/en-us/HT213811
[55] Source, Pixel Update Bulletin—June 2023. [Online]. Available: https://source.android.com/docs/security/bulletin/pixel/2023-06-01
[56] Mandiant, VMware ESXi Zero-Day Used by Chinese Espionage Actor to Perform Privileged Guest Operations on Compromised Hypervisors. [Online]. Available: https://www.mandiant.com/resources/blog/vmware-esxi-zero-day-bypass
[57] Acmesh, acme.sh Runs Arbitrary Commands from a Remote Server #4659, 2023. [Online]. Available: https://github.com/acmesh-official/acme.sh/issues/4659
[58] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop.html
[59] Progress, MOVEit Transfer Critical Vulnerability (May 2023). [Online]. Available: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[60] Emby, Emby Server does not start - Security Advisory 2023-05-25. [Online]. Available: https://emby.media/support/articles/advisory-23-05.html
[61] Barracuda, Barracuda Email Security Gateway Appliance (ESG) Vulnerability, 2024. [Online]. Available: https://www.barracuda.com/company/legal/esg-vulnerability
[62] Apple, About the Security Content of iOS 16.0. [Online]. Available: https://support.apple.com/en-us/HT213757

[63] Microsoft, CVE-2023-24932: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24932
[64] Microsoft, CVE-2023-29336: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336
[65] Samsung, Security Update. [Online]. Available: https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05
[66] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html
[67] Google, Stable Channel Update for Desktop, 2023. [Online]. Available: https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html
[68] Apple, About the Security Updates. [Online]. Available: https://support.apple.com/en-us/HT213720
[69] 3CX, DesktopApp Security Alert, 2023. [Online]. Available: https://www.3cx.com/blog/news/desktopapp-security-alert/
[70] Google, Spyware Vendors use 0-days and n-days Against Popular Platforms, 2023. [Online]. Available: https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/
[71] Korea Internet & Security Agency (KISA), 2023. [Online]. Available: https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&nttId=71023&menuNo=205020
[72] General Bytes, Security Incident March 17-18th, 2023. [Online]. Available: https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2885222430/Security+Incident+March+17-18th+2023
[73] Adobe, Security Updates Available for Adobe ColdFusion | APSB23-25, 2023. [Online]. Available: https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html
[74] Microsoft, CVE-2023-23397: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23397
[75] Microsoft, CVE-2023-24880: Security Advisory, 2023. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24880
[76] Fortinet, Analysis of FG-IR-22-369, 2023. [Online]. Available: https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis
[77] Microsoft, CVE-2023-21823: Security Advisory, 2023. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21823
[78] Microsoft, CVE-2023-23376: Security Advisory, 2023. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23376
[79] Microsoft, CVE-2023-21715: Security Advisory, 2023. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21715
[80] Apple, About the Security Content of iOS 16.3.1 and iPadOS 16.3.1. [Online]. Available: https://support.apple.com/en-us/HT213635
[81] Brain Krebs, [Post]. InfoSec Exchange. [Online]. Available: https://infosec.exchange/@briankrebs/109795710941843934
[82] Microsoft, CVE-2023-21674: Security Advisory, 2023. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21674