Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly September 2023

This report primarily analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from September 1 to 30, 2023. It includes the total number of vulnerabilities disclosed within the reporting period, the number of critical and zero-day vulnerabilities disclosed, the number of vulnerabilities actively exploited at the time of writing, and additional major trends and noteworthy vulnerabilities.

Key Findings

- In September 2023, an unprecedented 14 high-risk zero-day vulnerabilities affected Apple, Microsoft, Google, Adobe, Cisco, WordPress, Progress, and JetBrains products. This is the highest number of zero-day vulnerabilities that we have observed in the last 12 months.
- In threat campaigns that attracted the greatest attention from threat researchers, Google released emergency security updates to address 2 critical zero-day vulnerabilities in its Google Chrome web browser that, as of this writing, have been actively exploited in the wild to deploy Pegasus spyware.
- Apple patched 5 new zero-day vulnerabilities; 2 were used to deploy Pegasus spyware, while the other 3 were utilized for Predator spyware deployment. The vulnerabilities that threat actors exploited to deploy Pegasus were part of an exploit chain called "BLASTPASS" that enables threat actors to bypass Apple's BlastDoor Sandbox framework and compromise victims without user interaction. These vulnerabilities affected iPhones, iPads, Mac laptops, and Apple Watches.
- 22 of the approximately 2,100 vulnerabilities disclosed in September 2023 were high-risk, according to Recorded Future data.
- Microsoft patched 2 zero-day vulnerabilities in September 2023. These vulnerabilities affected Microsoft Office and 365 applications as well as Microsoft's Streaming Service Proxy.

CVE Monthly Prominent Vulnerability Disclosures

In an unprecedented month, we identified 22 newly disclosed vulnerabilities with high risk scores for September 2023, 14 of which were zero-day vulnerabilities, thus marking the highest number observed in both categories over the last 12 months. Apple was the vendor affected by the highest number of zero-day vulnerabilities, 5 of which were actively exploited to deploy the Predator and Pegasus spyware. 2 of the patched Apple zero-day vulnerabilities (CVE-2023-41991 and CVE-2023-41993) affect WebKit (a browser engine used by Apple). So far in 2023, Apple has patched a total of 13 zero-day vulnerabilities. Several of these were found in its WebKit, allowing threat actors to run malicious code to process crafted content and/or steal data.

According to our dataset, 2 zero-day vulnerabilities in the Google Chrome web browser, CVE-2023-4863 and CVE-2023-5217, and 1 vulnerability tracked as CVE-2023-20269 in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD), attracted significant attention from security researchers. This is likely due to threat actors' active exploitation of these 3 vulnerabilities. Threat actors have purportedly exploited CVE-2023-4863 and CVE-2023-5217 to deploy Pegasus spyware. Cisco stated that ransomware groups, including Akira, exploited CVE-2023-20269. As outlined in Recorded Future's H1 2023: Ransomware's Pivot to Linux and Vulnerable Drivers report, at the time of writing, Insikt Group posited that ransomware threat actors would continue to look for and exploit vulnerabilities in network security software to gain entry into victim systems when such activity allows them to launch attacks at a higher scale to increase profits. The exploitation of CVE-2023-20269 supports this argument and highlights the need for defenders to monitor network security software and promptly patch vulnerabilities.

The remaining zero-day vulnerabilities affected Apple, Microsoft, Google, Adobe, Cisco, WordPress, Progress, and JetBrains products. Further details about the zero-day vulnerabilities that were disclosed this month are highlighted below.

Apple Patched Zero-Day Vulnerabilities Used to Deploy Pegasus Spyware

Apple released patches for 2 actively exploited zero-day vulnerabilities on September 7 and 11, 2023. The 2 vulnerabilities are CVE-2023-41064, a buffer overflow flaw that can allow threat actors to execute arbitrary code on targeted devices via specially crafted images, and CVE-2023-41061, an input validation flaw that can also allow malicious actors to execute arbitrary code on victim devices via specially crafted malicious attachments. Threat actors are chaining the exploitation of these vulnerabilities to deploy Pegasus spyware, a malware developed by NSO Group, to target a civil society organization in Washington, DC. The US's Cybersecurity & Infrastructure Security Agency (CISA) added both vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on September 11, 2023, mandating timely patching for federal organizations. CISA stated in its notice that these types of vulnerabilities "pose significant risks to the federal enterprise".

Citizen Lab reported that the 2 flaws were chained in an attack sequence called "BLASTPASS." According to Citizen Lab, BLASTPASS is a zero-click attack chain, meaning threat actors can use this exploit chain to compromise victims without any user interaction.The attack abused PassKit, a framework for developers to integrate Apple Pay into their products, and BlastDoor, Apple's SandBox framework that is set up to prevent zero-click attacks. Citizen Labs initially discovered CVE-2023-41064 and disclosed the vulnerability to Apple; upon investigating the vulnerability, Apple discovered the other zero-day vulnerability used in the attack sequence, CVE-2023-41061. The vulnerabilities enabled threat actors to gain arbitrary code execution on iPhone and iPad devices.

Researchers at Citizen Lab and Apple urged organizations to promptly patch their devices to prevent the exploit chain using CVE-2023-41064 and CVE-2023-41061. Additionally, Apple recommends Lockdown Mode, an extreme security mode for Apple devices, as an extra security measure. In contrast to standard security features, Lockdown Mode is entirely discretionary and is designed for individuals facing an elevated risk of targeted attacks, such as high-profile figures like journalists, human rights defenders, government officials, or dissidents.

Apple Released Updates For 3 New Zero-Day Vulnerabilities

On September 21, 2023, Apple released emergency security updates to address 3 new zero-day vulnerabilities that were exploited in attacks targeting iPhone and Mac users. 2 of the vulnerabilities affect Apple's WebKit browser engine (CVE-2023-41993) and Security framework (CVE-2023-41991). If successfully exploited, these vulnerabilities can allow threat actors to "bypass signature validation using malicious apps or gain arbitrary code execution via maliciously crafted webpages". The third vulnerability (CVE-2023-41992) was found in the Kernel framework. If successfully exploited, it can allow threat actors who are already capable of executing code on the local system to further escalate privileges. Apple patched these vulnerabilities in its latest software updates, including for macOS, iOS, iPadOS, and watchOS, by fixing a certificate validation issue and implementing improved security checks.

Microsoft Released Patch for 2 Actively Exploited Vulnerabilities: CVE-2023-36802 and CVE-2023-36761

Microsoft's Patch Tuesday for September 2023 addressed 59 security vulnerabilities, including 2 actively exploited zero-day vulnerabilities. CVE-2023-36802 is a local privilege elevation vulnerability affecting Microsoft's Streaming Service Proxy that allows attackers to gain SYSTEM privileges. CVE-2023-36761 is a Microsoft Word Information Disclosure Vulnerability that can be used to steal NTLM hashes when opening a document, including in the preview pane. If threat actors gain access to these hashes, they can potentially masquerade as the user, gaining unauthorized access to sensitive data.

The US's CISA added these vulnerabilities to its KEV catalog on September 12, 2023. Federal agencies are required to patch the vulnerabilities by October 3, 2023.

Google Chrome and Mozilla Vulnerability, CVE-2023-4863, Actively Exploited in the Wild
On September 11, 2023, Google released an emergency security update to address a critical zero-day vulnerability, tracked as CVE-2023-4863, in its Google Chrome web browser. CVE-2023-4863 also affects Mozilla Firefox and Thunderbird. The vulnerability is a heap buffer overflow in the WebP Codec that allows remote code execution (RCE). Mozilla also rolled out security updates for Firefox and Thunderbird to fix the same zero-day vulnerability.

Google Addressed CVE-2023-5217 Vulnerability in Google Chrome Browser
On September 27, 2023, Google disclosed and patched a zero-day vulnerability affecting Chrome tracked as CVE-2023-5217, which threat actors reportedly exploited to deploy Pegasus spyware. This is the fifth zero-day vulnerability disclosed by Google in 2023.

CVE-2023-5217 is a high-severity vulnerability that arises from a heap buffer overflow flaw within the VP8 encoding of the open-source libvpx video codec library. If exploited, threat actors can engage in various malicious activities, such as causing application crashes, executing arbitrary code, and deploying additional malware.

Google patched CVE-2023-5217 by releasing an updated Google Chrome version (117.0.5938.132) for all global users on Windows, Mac, and Linux operating systems via the Stable Desktop channel. While the advisory noted that it could take days or weeks for the patched version to reach all users, BleepingComputer verified that the update was immediately available.

Cisco Warned Users of New Zero-Day Vulnerability Tracked as CVE-2023-20269
On September 6, 2023, Cisco issued a warning about a zero-day vulnerability, tracked as CVE-2023-20269, in its ASA and FTD products. The vulnerability results from improper separation of authentication, authorization, and accounting (AAA) between different features of the software. The vulnerability follows reports from Cisco stating that ransomware groups, including Akira, exploited this vulnerability and generally attempted to access Cisco VPNs without multi-factor authentication (MFA) as one of their initial access methods.

CVE-2023-20269 allows unauthorized remote threat actors to conduct brute-force attacks against existing accounts that do not have MFA enabled. As there are no limitations on the number of username and password attempts, threat actors are able to try an unlimited number of different password and username combinations until they gain access. After gaining access to targeted accounts, threat actors can establish a clientless SSL VPN session on the targeted device if the following conditions are met:

- The threat actor must have obtained valid credentials for a user present in either the LOCAL database or the AAA server used for HTTPS management authentication
- The device must be running Cisco ASA Software Release 9.16 or earlier
- SSL VPN must be enabled on at least 1 interface
- The DfltGrpPolicy must allow the clientless SSL VPN protocol

In the table below, actively exploited vulnerabilities affecting the 8 major software vendors are highlighted in gray.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
1	CVE-2023-41179	99	Trend Micro Apex One	A vulnerability in the third-party AV uninstaller module contained in Trend Micro Apex One that, if exploited, can allow a threat actor to execute arbitrary commands.	evil_minio	Yes
2	CVE-2023-41061	99	Apple iOS 16.6 iPadOS 16.6	An input validation flaw that can also allow malicious actors to execute arbitrary code on victim devices via specially crafted malicious attachments.	Pegasus	Yes
3	CVE-2023-41064	99	Apple iOS 16.6 iPadOS 16.6	A buffer overflow flaw that can allow threat actors to execute arbitrary code on targeted devices via specially crafted images.	Pegasus	Yes
4	CVE-2023-26369	99	Adobe Acrobat Reader Adobe Acrobat	An out-of-bounds write vulnerability that could result in arbitrary code execution.	N/A	Yes
5	CVE-2023-41992	99	Apple Kernel Framework	A privilege escalation vulnerability affecting the kernel framework that, if exploited, can lead to threat actors taking complete control over the affected device.	Predator	Yes
6	CVE-2023-41993	99	Apple Webkit Browser Engine	Bypass signature validation flaw that, if exploited, can allow for arbitrary code execution.	Predator	Yes
7	CVE-2023-41991	99	Apple Webkit Browser Engine	Bypass signature validation flaw that, if exploited, can allow for arbitrary code execution.	Predator	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
8	CVE-2023-36761	99	Microsoft Office Microsoft 365 Applications	This vulnerability can be used to steal NTLM hashes when opening a document, including in the preview pane.	N/A	Yes
9	CVE-2023-36802	99	Microsoft Streaming Service	This vulnerability is a local privilege elevation vulnerability that allows attackers to gain SYSTEM privileges.	N/A	Yes
10	CVE-2023-4863	99	Google Chrome Mozilla Firefox	The vulnerability is a heap buffer overflow in the WebP Codec that allows RCE.	Pegasus	Yes
11	CVE-2023-35674	99	Google Android Operating System	An error in the code has the potential to result in a local escalation of privilege without requiring any additional execution privileges. Notably, user interaction is not a prerequisite for successful exploitation.	N/A	Yes
12	CVE-2023-20269	99	Cisco ASA Cisco FTD	A vulnerability that results from improper separation of AAA. Unauthorized remote threat actors can conduct brute-force attacks against existing accounts that do not have MFA enabled.	LockBit, Akira	Yes
13	CVE-2022-34224	82	Adobe Acrobat Reader Adobe Acrobat DC Adobe Acrobat	A Use After Free vulnerability that could result in arbitrary code execution.	N/A	N/A
14	CVE-2022-34227	81	Adobe Acrobat	A Use After Free vulnerability that could result in arbitrary code execution.	N/A	N/A
15	CVE-2023-20252	81	Cisco SD-WAN	A vulnerability in the Security Assertion Markup Language (SAML) APIs of Cisco Catalyst SD-WAN Manager Software could	N/A	N/A

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
				allow an unauthenticated, remote threat actor to gain unauthorized access to the application as an arbitrary user.		
16	CVE-2023-5217	79	Google Chrome prior to 117.0.5938.132 libvpx 1.13.1 (Google)	A heap overflow vulnerability. If exploited, threat actors can engage in various malicious activities, such as causing application crashes, executing arbitrary code, and deploying additional malware.	Pegasus, Metasploit	Yes
17	CVE-2023-40044	79	Progress Software WS_FTP Server Ad hoc Transfer Module and Server manager	If exploited, allows a pre-authenticated attacker to execute remote commands on the underlying WS_FTP Server operating system for versions before 8.7.4 and 8.8.2.	N/A	N/A
18	CVE-2023-4634	79	WordPress media library assistant plugin	The vulnerability arises from inadequate controls on file paths in the “mla_stream_file” parameter, potentially enabling attackers to supply malicious files via FTP for directory lists and unauthorized code execution.	JokeFrom Mars	N/A
19	CVE-2023-4762	79	Google Chrome before version 116.0.5845.179	A type confusion vulnerability enabling remote attackers to execute arbitrary code by exploiting a crafted HTML page.	Predator	N/A
20	CVE-2023-38204	79	Adobe ColdFusion	A deserialization of Untrusted Data vulnerability that could result in arbitrary code execution.	N/A	Yes
21	CVE-2023-38146	79	Windows 11 Themes	A high-severity vulnerability discovered in Windows 11 Themes that allows an attacker to remotely execute	N/A	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
				arbitrary commands when a user loads a ".theme" file.		
22	CVE-2023-42793	79	JetBrains TeamCity before 2023.05.4	An authentication bypass that, if exploited, allows threat actors to conduct RCE and gain administrative control of a TeamCity Server.	N/A	N/A

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.