Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly September 2022

This report analyzes the top vulnerabilities disclosed across 8 major software vendors (Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco) from September 1 to September 30, 2022. This report examines 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 Judgments

- In September 2022, a number of trends in vulnerability exploitation saw continued development: exploitation of Microsoft Exchange servers, zero-days in Apple and Google products, exploitation of QNAP software by Deadbolt ransomware, attacks against endpoint management products from vendors like Trend Micro and VMWare, and compromise of WordPress plugins.
- Similar to August 2022, operating systems were a recurring target of exploitation, but otherwise products with high-risk or exploited vulnerabilities were a fairly mixed bag of mail servers, security agents, firewall modules, templating engines, and web browsers.
- The number of zero-days disclosed in September was higher than in August (7 vs. 3) and is in line with a trend since 2021 of zero-days comprising the majority of newly disclosed and exploited vulnerabilities.

CVE Monthly Prominent Vulnerability Disclosures

September 2022 featured many instances of "next verse, same as the first" for vulnerability exploitation. At the tail end of September, Microsoft confirmed exploitation of 2 zero-day vulnerabilities in its Microsoft Exchange products, dubbed "ProxyNotShell" due to their similarity to the ProxyShell vulnerabilities of 2021. Among other major vendors we track, Apple and Google released reports of zero-day vulnerability exploitation affecting their iOS and Chrome products, respectively. In Apple's case, it was the 8th zero-day vulnerability they have disclosed so far in 2022, and in Google's case, it was at least the 4th such disclosure. Outside of our prioritized vendors, but still affecting many users, QNAP reported that a Deadbolt ransomware campaign was yet again exploiting a vulnerability in its software (in particular, its Photo Station offering). Trend Micro similarly reported that criminals were exploiting a zero-day vulnerability in its Apex One security agent, which is not only part of an ongoing trend of attacks against vulnerabilities in endpoint management (for example, against VMWare Workspace) but is also part of a multi-year trend of criminals targeting Apex One. Finally, WordPress reported millions of exploitation attempts against a vulnerability in its WPGateway plugin barely a week after news of exploitation of a separate plugin.

Occurring right at the end of the month, 2 Microsoft zero-day vulnerabilities are likely to be the priority for defenders and researchers going into October. On September 29, Microsoft researcher Kevin Beaumont shared on social media that "a new zero day exists in Microsoft Exchange, and is actively being exploited in the wild". This news was based on a prior blog from Vietnamese cybersecurity company GTSC in which researchers identified ProxyShell-like exploitation of a Microsoft Exchange server which was already patched for the ProxyShell vulnerabilities that were disclosed in 2021. Within 24 hours, the initially reported zero-day had doubled to 2, which were assigned the identifiers of CVE-2022-41040 and CVE-2022-41082 (and the nickname "ProxyNotShell" by Beaumont). Closing the cycle out, at least for now, Microsoft published a blog on September 29 in which they confirmed that they were working on an "accelerated fix" for the vulnerabilities, that customers of their Microsoft Exchange Online offering did not need to take action, and that customers with on-premises Microsoft Exchange servers could implement a set of URL Rewrite Instructions and "block exposed Remote PowerShell ports".

Early in the month, Google released an emergency patch for CVE-2022-3075, a vulnerability in its Chrome web browser caused by insufficient data validation in Mojo. As is typical for Google, the

company released few details about the attackers or victims associated with the exploitation. Then on September 12, 2022, Apple released security updates to address a newly discovered zero-day security flaw found in its macOS and iOS devices tracked as CVE-2022-32917. Reported to Apple by an anonymous researcher, the vulnerability may allow malicious applications to execute arbitrary code with kernel privileges. If a vulnerability affects 1 Apple product line, it probably affects them all: the vulnerability affects iPhone 6s and later; all models of iPad Pro; iPad Air 2 and later; iPad 5th generation and later; iPad mini 4 and later; and iPod touch (7th generation). In addition, it affects Mac desktops or MacBooks running macOS Big Sur 11.7 and macOS Monterey 12.6.

On September 3, 2022, QNAP disclosed in a security advisory their discovery of a campaign involving the DeadBolt Ransomware, in which threat actors exploited a recently disclosed vulnerability tracked as CVE-2022-27593 to target vulnerable devices, specifically QNAP NAS devices running Photo Station. Successful exploitation of the vulnerability could allow threat actors to modify system files. QNAP devices have been targeted by threat actors in the past, with various ransomware strains infecting such devices, such as Muhstik, QLocker, eCh0raix, and AgeLocker. The importance of high-quality photo storage for businesses, particularly businesses with a heavy social media presence, is likely a factor in DeadBolt's targeting of Photo Station. However, given the group's targeting of QNAP in the past, the greatest factor behind this new vulnerability exploitation is almost certainly the group's attention to QNAP products in general.

On September 13, 2022, Trend Micro released security updates to address several security flaws found in its Apex One and Apex One as a Service (SaaS) endpoint protection offerings. The first vulnerability, tracked as CVE-2022-40139, is an improper validation of rollback mechanism components. If exploited, the vulnerability would allow an adversary with administrative access to the Apex One server to instruct the affected software clients to download an unverified rollback package, leading to remote code execution. Trend Micro notes that the adversary would need Apex One administrator console access to exploit this vulnerability, which makes this vulnerability slightly harder to exploit for threat actors. However, Trend Micro also disclosed in its security update that it has observed CVE-2022-40139 being exploited in the wild. Endpoint protection and identity/access management software has been a notable target of threat actors in 2022 as exemplified by exploitation of vulnerabilities in products associated with VMWare Workspace.

Finally, a vulnerability associated with probably the highest (reported) volume of attempts at exploitation in September 2022 is CVE-2022-3180, which affects a WordPress plugin designed to assist with site administration. Per open sources, WordPress reported that it blocked nearly 5 million attacks against almost 300,000 WordPress sites running vulnerable software. Given the over 400 million sites that run WordPress, this is an almost imperceptible percentage of the total space for WordPress compromise, but it still represents a critical security risk for many site administrators.

In the table below, vulnerabilities associated with the list of major vendors we have prioritized are highlighted.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-3180	99	WordPress WPGateway	Administration plugin		Yes
CVE-2022-31814	93	Microsoft Windows	Security service		No
CVE-2022-37969	89	Microsoft Windows	Directory service (Active Directory)		No
CVE-2022-27593	79	Cisco IOS XR	Network operating system		Yes
CVE-2022-34721	79	Microsoft Windows	Printer operations		No
CVE-2022-37767	76	Apple AppleAVD	Audio and video decoding		No
CVE-2022-3075	64	Apple macOS	Graphics driver		Yes
CVE-2022-32917	64	Atlassian Confluence	Collaborative software		Yes

Recorded Future®

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 intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.