Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly May 2022

This report analyzes the top vulnerabilities disclosed across 8 major software vendors, including Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco, from May 12 to June 6, 2022. This report 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 worth highlighting.

Key Judgments

- Several zero-day vulnerabilities, or vulnerabilities being exploited very soon after disclosure, are currently affecting a wide array of products and software, including remote support tools, operating systems, Active Directory services, and graphics driver spaces. These vulnerabilities affect products from major vendors like Microsoft, Apple, and Cisco.
- Of the 7 critical vulnerabilities disclosed this past month, 5 were zero-days when disclosed. In widely used software from Microsoft, Apple, and Cisco, there has been no time to patch before attackers target these vulnerabilities, so mere vulnerability management alone is not sufficient. Security teams are strongly encouraged to deploy a defense-in-depth approach across their networks.
- For the most prominent of these vulnerabilities, CVE-2022-30190 (aka "Follina"), Insikt Group observed exploitation by the China-linked threat group TA413 on May 30, barely a day after the vulnerability had initially been disclosed. It was also later confirmed that the vulnerability was used in 3 threat actor campaigns prior to public disclosure, including a spearphishing campaign targeting entities in Saudi Arabia. The exploitation before disclosure shows how quickly APT groups take advantage of major new exploits.
- A key takeaway from the Follina disclosure is how fast attackers are using maldoc-based exploits now that Microsoft is turning off VBA-based macros by default. Security teams should prepare themselves for an eventful second half of the year as additional ways that Microsoft systems are vulnerable to maldoc exploits are likely to be discovered.
- Users of Cisco's IOS XR product face a serious vulnerability in CVE-2022-20821, a security flaw in the health check remote patient monitoring (RPM) that may allow an unauthenticated adversary to remotely access the Redis instance that is running within the NOSi docker container.
- Apple MacOS and iOS users should be aware of CVE-2022-22674 and CVE-2022-22675. Apple alleged that both vulnerabilities may be under active exploitation and has already released urgent patches for the vulnerabilities. The company urges users to upgrade to the latest versions of the software to mitigate potential threats.
- Outside of the main vendors highlighted in this report, security teams should also be aware of CVE-2022-26134, a critical unauthenticated remote code execution vulnerability found in Confluence Server and Data Center that installs web shells.

CVE Monthly Prominent Vulnerability Disclosures

This month, newly disclosed critical vulnerabilities associated with 8 major software vendors, including Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco, were disclosed across a number of popular technologies. From the Recorded Future Platform and open source (OSINT) data, we determined the total volume of vulnerabilities disclosed across these vendors in May 2022, the number of critical vulnerabilities disclosed, how many of these critical vulnerabilities were zero-days, and any instances of active exploitation in the wild. In May 2022, 154 vulnerabilities were disclosed across the 8 major software vendors identified above, 7 of which carry a "Critical" CVSS score. Of the 7 critical vulnerabilities highlighted this month, 5 were zero-day vulnerabilities. At the time of writing, Recorded Future data indicates that all 7 critical vulnerabilities disclosed this month have been exploited in the wild, so security teams deploying the affected technologies should prioritize these vulnerabilities for patching.

As the data suggests, vulnerabilities disclosed this month are spread across a number of technologies, including remote support tools, operating systems, Active Directory services, and graphics driver spaces. The 3 vendors most affected by critical and zero-day vulnerabilities in May were Microsoft, Cisco, and Apple. Due to the fact that the majority of the critical vulnerabilities disclosed this month were zero-days, defenders did not have adequate time to patch these vulnerabilities before they were targeted by threat actors. Therefore, routine vulnerability and patch management is not an effective solution to protect organizations against exploitation of these vulnerabilities; a defense-in-depth approach is the most effective solution across networks.

For the most prominent of these vulnerabilities, CVE-2022-30190 (Follina), Insikt Group observed exploitation by the China-linked threat group TA413 on May 30, barely a day after the vulnerability had initially been disclosed. It was also later confirmed that the vulnerability was used in 3 threat actor campaigns prior to public disclosure, including a spearphishing campaign targeting entities in Saudi Arabia. The exploitation before disclosure shows how quickly APT groups take advantage of major new exploits.

Follina represents a serious concern for Microsoft, considering it recently announced that VBA-based macros would be disabled by default. Security researcher Kevin Beaumont detailed how Follina can allow a vulnerable Windows instance to be made to execute Powershell code from a maldoc via the Windows support command **`msdt`** as implemented on a remote HTML file, even when macros were disabled. After the success of Follina, threat actors are sure to find novel ways of deploying maldoc-based exploits in spite of Microsoft disabling macros by default. In the second half of 2022, this could lead to security researchers and threat actors alike discovering a variety of new ways Microsoft systems are vulnerable to maldoc exploits.

As for Cisco vulnerabilities disclosed this month, users of their IOS XR product should verify that they have the proper steps in place to mitigate the risk associated with CVE-2022-20821. CVE-2022-20821 is a security flaw in the health check remote patient monitoring (RPM), which may allow an unauthenticated adversary to remotely access the Redis instance that is running within the NOSi docker container. According to Cisco, the vulnerability affected Cisco 8000 Series Routers running a vulnerable release of Cisco IOS XR Software and had the health check RPM installed and active. Cisco provided workarounds to address the security flaw, including disabling the health check, explicitly disabling the use cases, and using an Infrastructure Access Control List (iACLs) to block port 6379. Individuals should administer the applicable workaround or update their software to the latest version to avoid further exploitation.

Finally, Apple owners should ensure they are running the most recent version of MacOS Monterey and iOS to mitigate the risks associated with CVE-2022-22674 and CVE-2022-22675. CVE-2022-22675 is an out-of-bounds write vulnerability affecting the audio and video component called AppleAVD, which allows execution of binary codes with kernel privileges. CVE-2022-22674 is an out-of-bounds read vulnerability affecting the Intel Graphics Driver module that could lead to disclosure of the kernel memory. Affected products and versions include the following:

- MacOS Monterey
- iPhone 6s and later
- All models of iPad Pro, iPad Air 2 and later, iPad 5th Gen and later, iPad mini 4 and later, and iPod touch 7th Gen

Apple alleged that both vulnerabilities may be under active exploitation and has already released urgent patches for the vulnerabilities. The company has urged Apple users to upgrade to the latest versions of the software to mitigate potential threats.

A vulnerability worth highlighting this month that affected products outside of those released by the 8 major software vendors identified in this report is CVE-2022-26134, a critical unauthenticated remote code execution vulnerability found in Confluence Server and Data Center that installs web shells. The vulnerability was disclosed in a report by Volexity, who discovered the vulnerability during an incident response investigation with their customers running the Atlassian Confluence Server application. Volexity and Atlassian have not described the nature of the flaw and Insikt Group has not identified any public proofs of concept at the time of this writing. However, Atlassian warns users that the vulnerability is actively exploited and recommends security teams push the latest patch update for Confluence, published June 2 on Confluence's website.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-30190	99	Microsoft Windows	Remote support tool	Turian backdoor	Yes
CVE-2022-26925	99	Microsoft Windows	Security service		Yes
CVE-2022-26923	99	Microsoft Windows	Directory service (Active Directory)		No
CVE-2022-20821	99	Cisco IOS XR	Network operating system		Yes
CVE-2022-29104	93	Microsoft Windows	Printer operations		No
CVE-2022-22675	89	Apple AppleAVD	Audio and video decoding		Yes
CVE-2022-22674	89	Apple macOS	Graphics driver		Yes
CVE-2022-26134	79	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.