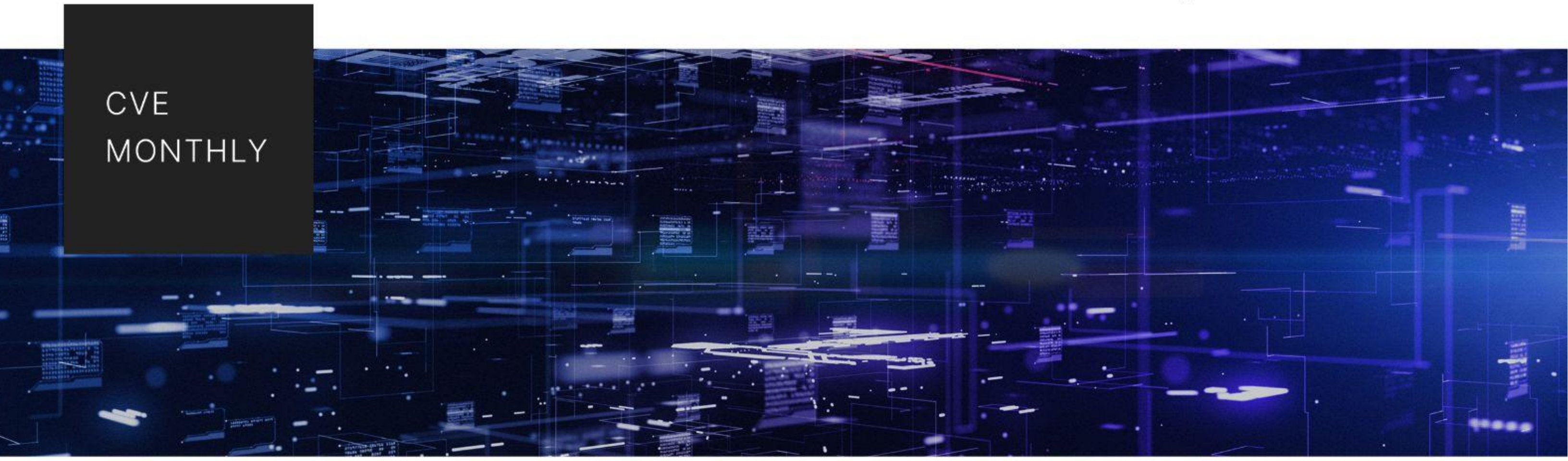
Recorded Future®



CVE MONTHLY

Recorded Future CVE Monthly October 2022

This report analyzes the top vulnerabilities disclosed across 8 major software vendors, including Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco, from October 1 to October 31, 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

- Recorded Future identified 8 newly disclosed vulnerabilities with high risk scores for October 2022, at least 4 of which are zero-day vulnerabilities, affecting Apple, Fortinet, Google, and Microsoft. The Mark-of-the-Web (MOTW) vulnerabilities that affect recent versions of Microsoft Windows and Windows Server have not yet been assigned CVE identifiers but have also reportedly been exploited in the wild.
- The MOTW vulnerabilities will almost certainly see a rapidly increasing set of threat actor exploitation due to their severity; security researcher and vendor details have been sparse due to fears of the vulnerabilities' exploitation at scale.
- Newly disclosed vulnerabilities in Apache ("Text4Shell", named in the same style as the separate flaw "Log4Shell") and OpenSSL are very likely less severe than initially considered on first reporting.

CVE Monthly Prominent Vulnerability Disclosures

Of the trends in the critical vulnerability landscape in October 2022, probably the most interesting was the number of flaws that subverted expectations, being either not as bad, or worse, than originally thought. The newly disclosed vulnerabilities that picked up the most press (including the MOTW vulnerabilities in Microsoft Windows, the "Text4Shell" vulnerability affecting Apache Commons Text, and the 2 initially critical vulnerabilities in OpenSSL) all had an initial assessment that grew either more or less severe as more information was released by their respective researchers. Since the MOTW vulnerabilities do not yet have CVE identifiers, they do not appear in the table at the end of this report, but as they have been exploited in the wild, they bring our accurate tally of newly disclosed and exploited vulnerabilities for this month to 10, with at least 4 of these being zero-day vulnerabilities (for Apple, Fortinet, Google, and Microsoft).

The Text4Shell and OpenSSL vulnerabilities raised the specter of widespread, nasty exposure when first announced, the former due to its obvious potential associations with Log4Shell, and the latter due to its historic associations with flaws like HeartBleed. However, these have turned out to be a little less worrisome due to much narrower conditions for exploitation. On the other hand, many details about the MOTW vulnerabilities, which researcher Will Dormann first reportedly disclosed to Microsoft in July 2022, have still not been released due to Dormann's fear of how ubiquitous exploitation might be if the bug were understood by a large set of threat actors.

There are echoes of Follina in the 2 MOTW vulnerabilities, since, as former Microsoft researcher Kevin Beaumont has noted, it allows cyberattackers to make malicious "macros work in Office despite the Office macro changes" (alluding to Microsoft's initiative to turn off macros by default). And there are echoes of effectively every exploit application for 2022: the use of MOTW in ransomware campaigns. In particular, security researchers from HP revealed on October 12, 2022, that 1 of the 2 MOTW flaws had been exploited by threat actors to deploy the Magniber ransomware to target home users with fake Windows 10 or antivirus updates. Beaumont has additionally said that "if Emotet/Qakbot/etc find [how to use MOTW] they will 100% use it at scale". Given these attributes — highly flexible and already exploited — network defenders should prioritize MOTW mitigation if they have not already. There is an initial (unofficial) patch from 0patch, released on October 17, for Windows Server 2008 through Windows 11. As of this writing, though, Microsoft has not yet released its own set of patches or CVE identifiers.

Text4Shell is the first of the “not as bad as you thought” vulnerabilities for October 2022, likely to many defenders’ relief. On October 13, 2022, Apache developers disclosed a critical remote code execution (RCE) vulnerability, tracked as CVE-2022-42889, found in the Apache Commons Text library. The security flaw, dubbed “Text4Shell” due to its similarities to the infamous Log4Shell (CVE-2021-44228) vulnerability, can be exploited to process untrusted data, which may lead to remote code execution. However, in a skeptical analysis of CVE-2022-42889 on October 17, 2022, researchers from Rapid7 posited that while the vulnerability in Apache’s Commons Text deserves attention, the similarities drawn between Log4Shell and Text4Shell are overstated. While in theory the Text4Shell vulnerability affects countless users, in practice it affects a much smaller subset of individuals than Log4Shell. According to Rapid7, unlike Log4Shell, where vast numbers of users were running vulnerable versions of Apache’s Log4j library, users are much more seldom to be seen running applications that pass malicious strings through the specific vulnerable “StringSubstitutor.createInterpolator()” method in the Commons Text library.

Similarly, and perhaps more directly, the now-finally-disclosed OpenSSL vulnerabilities (CVE-2022-3602 and CVE-2022-3786) have undergone a clear path from Critical to High in severity, after review by multiple users and researchers. The OpenSSL project released an updated version of OpenSLL (version 3.0.7) on November 1, 2022, to address 2 high-severity buffer overflow vulnerabilities in the OpenSSL open-source cryptographic library. Previously, on October 25, 2022, OpenSSL warned organizations to scan their environments for vulnerable OpenSSL instances in preparation for the release of OpenSSL version 3.0.7. Both vulnerabilities affect the X.509 certificate verification mechanism in OpenSSL.

Before the release of the updated patches by OpenSSL, security researchers warned and also anticipated that the 2 vulnerabilities “could have been the most serious vulnerabilities the industry has seen in more than a decade”, with researchers from CheckPoint noting that “[the] potential magnitude of [these] vulnerabilities is enormous”. However, soon after the patches for these vulnerabilities were released, OpenSSL stated in their most recent blog that they had “downgraded” the vulnerabilities’ severity level from “Critical” to “High”, due to some fairly specific conditions, such as the lack of common stack overflow mitigation and the lack of available vulnerable devices.

Outside of these attention-getters, several other vulnerabilities did see exploitation and are likely still a priority for defenders to address. The Fortinet zero-day vulnerability CVE-2022-40684, which affects FortiOS, FortiProxy, and FortiSwitchManager, was disclosed by Fortinet on October 10, 2022, with the warning that it was already being exploited in the wild. Fortinet vulnerabilities are a popular target for threat actors, given that successful exploitation has historically allowed them to gain initial access and move laterally within a target system’s environment. The US CISA has listed a number of Fortinet vulnerabilities, including CVE-2022-40684, in their Known Exploited Vulnerabilities Catalog.

Additionally, as has been a trend for a few months, Apple, Google, and Microsoft all disclosed zero-day vulnerabilities affecting their iOS (CVE-2022-42827), Chrome (CVE-2022-3723), and Windows (CVE-2022-41033) products, respectively. All 3 merely disclosed and patched without longer descriptions of the bugs outside of the note that they have been exploited in the wild.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-3723	99	Google Chrome	Web browser		Yes
CVE-2022-40684	99	Fortinet FortiOS, FortiProxy, FortiSwitchManager	Operating system, web proxy, network management		Yes
CVE-2022-41033	99	Microsoft Windows, Windows Server	Operating system		Yes
CVE-2022-41043	99	Microsoft Office	Document processor		No
CVE-2022-42827	99	Apple iOS, iPadOS	Operating system		Yes
CVE-2022-3602	79	OpenSSL	Secure networking application		No
CVE-2022-42889	79	Apache Commons Text	Code library		No
CVE-2022-31678	74	VMWare Cloud Foundation, NSX Data Center	Cloud platform		No

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.