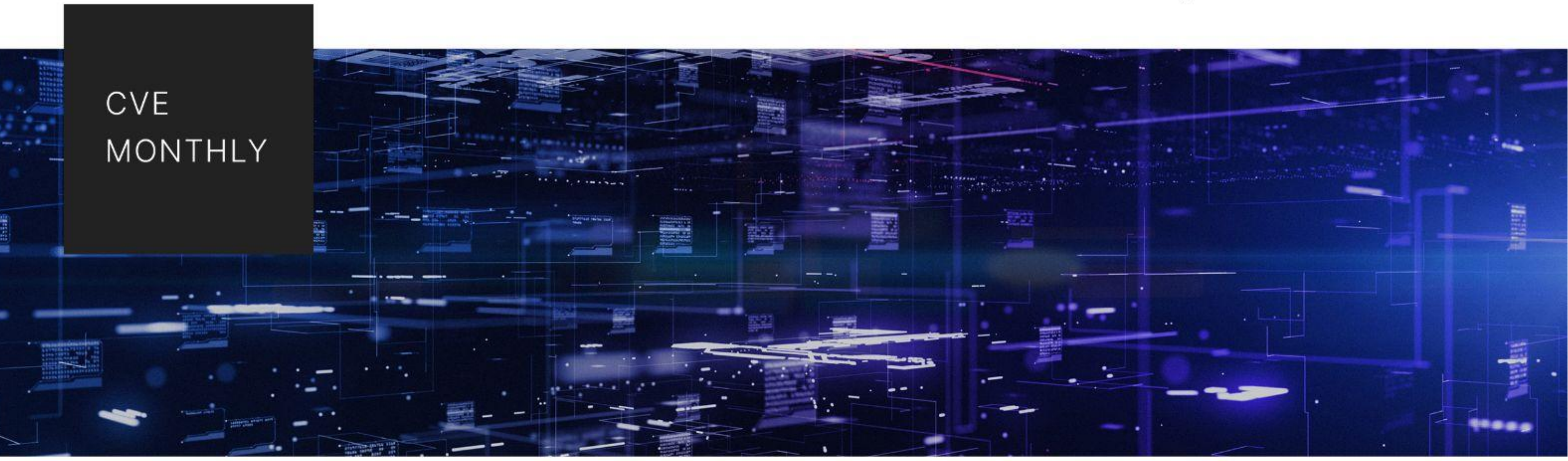
CVE
MONTHLY



Recorded Future CVE Monthly November 2022

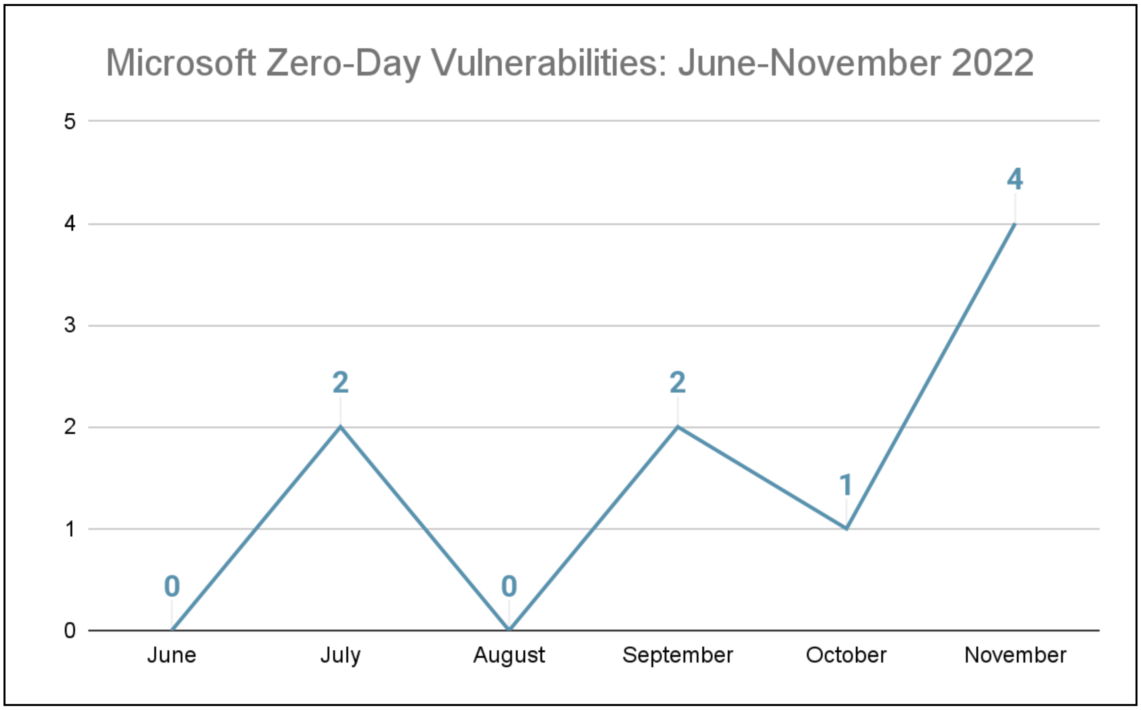
This report analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from November 1 to November 30, 2022. This report includes the total number of vulnerabilities disclosed within the reporting period, the number 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 9 newly disclosed vulnerabilities with high risk scores for October 2022, at least 6 of which are zero-day vulnerabilities, affecting Atlassian, Fortinet, Google, Grafana, and Microsoft. The most serious of these are almost certainly the 2 Mark-of-the-Web (MOTW) vulnerabilities that first received prominent coverage in October 2022.
- Microsoft vulnerabilities accounted for over half of our list this month, reflecting several disclosures of critical and already-exploited vulnerabilities affecting multiple components of Windows systems, including Print Spooler and Scripting Languages.
- Google's disclosure of a Chromium zero-day vulnerability is almost certainly a serious matter beyond Chrome users since several web browsers rely on Chromium technology.
- Newly observed exploitation of previously disclosed Microsoft and Oracle vulnerabilities demonstrates that while zero-day vulnerabilities are severe, there are many timeframes within which critical vulnerabilities can be exploited.

CVE Monthly Prominent Vulnerability Disclosures

There is a term from agriculture, "bumper crop", which refers to a season of especially high yield for a harvest. It is also one of the few phrases that accurately sums up the situation for Microsoft vulnerabilities in November 2022. Given its dominance as an operating system for both individual users and corporate environments, Microsoft Windows is consistently a target for vulnerability exploitation, but the bumper crop of zero-day vulnerabilities associated with Microsoft Windows in November 2022 was surprising even in the midst of a year of high-profile and often high numbers of zero-days. And while Microsoft was not the only major vendor to see zero-day exploitation (Google reported its eighth zero-day for the year), it certainly outweighed Google this month with 4 zero-days and another 1 vulnerability exploited shortly after disclosure. As if to balance things out, Apple, which has appeared in several of the last CVE Monthly reports, disclosed no exploited vulnerabilities this month.



As the chart above demonstrates, November 2022 was an unusually rough month for Microsoft zero-day disclosure, accounting for nearly as many zero-days as had been disclosed in the preceding 5 months put together. In particular, the MOTW vulnerabilities — a set of nasty vulnerabilities that allow malware to bypass Microsoft's ability to detect files downloaded from the internet — went from a generally unclear but heavily warned-against threat in October 2022 to an infection vector for ransomware and botnets in November 2022. These vulnerabilities are identified as CVE-2022-41049 and CVE-2022-41091. HP reported that criminals distributing the Magniber ransomware were exploiting CVE-2022-41091, and BleepingComputer reported on multiple episodes of exploitation, including 1 that spread Qbot malware. Given Qbot's links to follow-on ransomware attacks, its adoption of MOTW vulnerability exploitation should prompt network defenders to fix these vulnerabilities as soon as possible.

As part of its ongoing Patch Tuesday releases, Microsoft also reported exploitation of 3 other zero-day vulnerabilities: CVE-2022-41073 (affecting Windows Print Spooler, and bringing back unhappy memories of PrintNightmare from 2021); CVE-2022-41125 (affecting Cryptographic Next Generation [CNG] key isolation); and CVE-2022-41128 (affecting Windows Scripting Languages). Microsoft released fixes for 2 ProxyNotShell vulnerabilities (CVE-2022-41040 and CVE-2022-41082) as well, although these have been known since September 2022. The combination of remote code execution (RCE) vulnerabilities like CVE-2022-41128 with elevation-of-privilege vulnerabilities like CVE-2022-41073 exposes organizations to multiple modes of attack. If there is any silver lining on the Microsoft front this month, it is that, so far as is known, there was not yet another series of vulnerabilities in Microsoft Exchange that saw exploitation by nation-state groups.

Google, meanwhile, patched CVE-2022-4135, an RCE zero-day vulnerability in the Google Chrome browser, after adversaries started exploiting it in the wild. The vulnerability, which is the eighth zero-day in Google Chrome in 2022, causes heap buffer overflow in Google Chrome versions 107.0.5304.141, 107.0.5304.121, and 107.0.5304.122. Google's Threat Analysis Group identified the vulnerability a few days prior to larger news of adversary exploitation.

Google urged users to upgrade their Chrome browsers to version 107.0.5304.121 on macOS and Linux and 107.0.5304.121/.122 on Windows operating systems. Web browsers like Microsoft Edge, Brave, Opera, and Vivaldi are also vulnerable to exploits of this flaw because they are Chromium-based, which means that, ironically, Google's disclosure added at least 1 more zero-day vulnerability to the list of those that Microsoft defenders need to worry about.

The remaining vulnerabilities in our list below are associated with less well-known software developers, but should still receive attention. CVE-2022-38374 and CVE-2022-43781 were disclosed this month for Fortinet and Atlassian, respectively, and both of these vendors have seen critical vulnerability exploitation in 2022 already. Notably, CVE-2022-38374, which affects Fortinet's FortiADC line of hardware for managing application authentication and authorization, is the type of vulnerability that is attractive to criminals or nation-state groups looking to compromise a key piece of network infrastructure.

A couple of "honorable mentions" are also worth including for this month's analysis. First, in late November 2022, the US Cybersecurity and Infrastructure Security Agency (CISA) warned of exploitation of a RCE vulnerability in Oracle Access Manager, CVE-2021-35587, by adding it to its Known Exploited Vulnerabilities (KEV) Catalog on November 28, 2022. The active exploitation of the vulnerability follows the disclosure of proof-of-concept (POC) exploits for the vulnerability, which have been available for "several months", according to SecurityWeek. GreyNoise additionally reported that exploit activity was first recorded in September 2022, with an uptick in activity since then.

Second, as reported by CYFIRMA in late November 2022, threat actors have been exploiting a critical RCE vulnerability (CVE-2022-34721) in Windows Internet Key Exchange (IKE) protocol extensions belonging to organizations in retail, government, finance, and information technology (IT), since early September 2022. CYFIRMA researchers attributed this exploit campaign to an unknown Chinese threat group, based on an unspecified Chinese-language indicator observed in the campaign, specifically the phrase "流血你" ("bleed you").

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-4135	99	Google Chrome	Web browser		Yes
CVE-2022-41091	99	Microsoft Windows and Windows Server	Operating system	Magniber ransomware, Qbot	Yes
CVE-2022-41128	99	Microsoft Windows and Windows Server	Operating system		Yes
CVE-2022-41049	99	Microsoft Windows and Windows Server	Operating system		No

CVE-2022-41073	99	Microsoft Windows and Windows Server	Operating system		Yes
CVE-2022-41125	99	Microsoft Windows and Windows Server	Operating system		Yes
CVE-2022-38374	93	Fortinet FortiADC	Web application authentication / authorization		No
CVE-2022-39307	92	Grafana	Data visualization platform		No
CVE-2022-43781	76	Atlassian Bitbucket	Source code hosting		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.