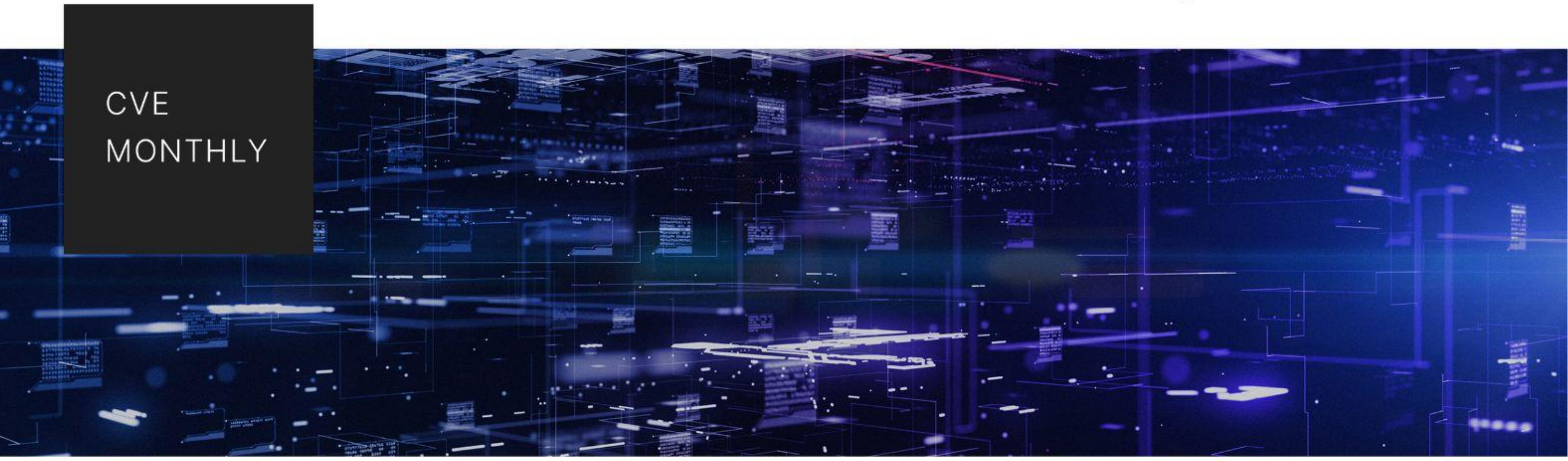

Recorded Future CVE Monthly December 2022

This report analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from December 1 to December 31, 2022. 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 worth highlighting.

Key Judgments

- Recorded Future identified 9 newly disclosed vulnerabilities with high risk scores for December 2022, at least 5 of which are zero-day vulnerabilities, affecting Apple, Citrix, Fortinet, Google, Microsoft, Cisco, and a few open-source software modules. The most serious of these are likely a vulnerability in Citrix (CVE-2022-27518) and in Microsoft (CVE-2022-44698).
- Enterprise-grade products continue to be targeted by vulnerability exploitation from advanced threat groups; such products include Citrix's ADC and Gateway solutions and Fortinet's FortiOS operating system.
- Microsoft's Windows operating system and Google's Chrome browser continue to see new vulnerability exploitation, as befits their respective high market saturation.

CVE Monthly Prominent Vulnerability Disclosures

"Is … that it?" After the spike in Microsoft zero-day disclosures last month, and certainly after the last 2 Decembers in which security defenders had to contend with the SolarWinds and then the Log4Shell software supply-chain crises, vulnerability disclosures in December 2022 felt tame by comparison. However, there were still high-profile vulnerabilities associated with active or advanced threat campaigns. The 2 vulnerabilities that attracted some of the highest attention were: CVE-2022-27518, a remote code execution (RCE) vulnerability affecting Citrix that has been exploited by a China-nexus threat group; and CVE-2022-44698, another in a series of Mark-of-the-Web bypass vulnerabilities making trouble for Microsoft users in 2022. A smattering of zero-day vulnerabilities also affected Apple's Webkit, Google Chrome, and Fortinet FortiOS. There are limited details on attackers or follow-on threat activity associated with exploitation of these vulnerabilities, aside from an unconfirmed report that CVE-2022-42475 in FortiOS has been exploited by an (as-yet-unnamed) ransomware group. On the whole, though, no vulnerability in the past month has (yet) had the severity or bonanza exploitation of Log4Shell in late 2021, and for that, security practitioners can be grateful.

The vulnerability with the most buzz in December 2022 was likely CVE-2022-27518, a vulnerability in Citrix ADC and Gateway products that the US National Security Agency (NSA) reported to have been exploited by Chinese group APT5 based on overlapping tactics, techniques, and procedures (TTPs) used in these recent attacks and previous APT5 campaigns. A separate advisory from Citrix confirmed that the organization had seen exploitation of the vulnerability in a "small number of targeted attacks". APT5 has historically focused on compromising network appliances and their associated software with the intent to target telecommunications, technology, and manufacturing organizations. Critical vulnerability exploitation is nothing new to the group, either: in April 2021, Mandiant researchers reported on APT5 exploiting a newly patched zero-day vulnerability in Pulse Connect Secure gateways, CVE-2021-22893, to deploy malware, collect credentials, and steal proprietary data from US Defense Industrial Base (DIB) networks.

Another vulnerability in an enterprise-grade product that saw exploitation in December 2022 was CVE-2022-42475, an SSL VPN pre-authentication vulnerability affecting Fortinet's FortiOS software suite. While Fortinet's initial advisory did not disclose details about active exploitation (except to say that it had occurred), security researcher Kevin Beaumont stated that a ransomware group was responsible for zero-day exploitation, although he did not provide further sourcing to validate this claim. Even more intriguingly (and frustratingly short on detail), Beaumont claimed that some of the malicious IPs released by Fortinet in association with exploit activity "look nation state related" and added that "not all ransomware is truly a ransom", implying that nation-state APT groups have exploited CVE-2022-42475 to deploy so-called ransomware on victim systems, calling to mind fake-ransomware-actual-wiperware like Azov and CryWiper. Regardless of these possibilities, at least 1 ransomware group in the last few years has targeted a FortiOS vulnerability: in August 2021, criminals affiliated with the LockBit ransomware gang exploited CVE-2018-13379 to gain initial access to specific victim networks.

Microsoft, it seems, cannot avoid going more than a few quarters these days without running into a months-long series of vulnerability disclosures with snappy group names: PrintNightmare, ProxyShell (then ProxyNotShell), and now the Mark-of-the-Web (MotW) vulnerabilities. After the disclosures of CVE-2022-41049 and CVE-2022-41091 back in November, the company disclosed a third MotW vulnerability, CVE-2022-44698, which was originally discovered by security researcher Will Dormann (also behind the discovery of the original MotW set). Threat actors can bypass MotW protections (designed to spot files downloaded from the internet) by creating ZIP archives, from which extracted files will not be marked with the MotW designation. Dormann has noted that optical disk image (ISO) files are particularly at risk of abuse via this vector, since MotW is not applied to them. Nor is this a hypothetical threat: as reported by Kaspersky in late December 2022, the North Korea-aligned BlueNoroff Group has delivered new strains of custom malware via malicious ISO and virtual hard disk (VHD) files by way of MotW bypass.

It also wouldn't be a month in 2022 without a few zero-day disclosures, absent much campaign or attacker detail, from Apple and Google. The latter issued a vulnerability announcement and patch for CVE-2022-4262, a type-confusion flaw in Chrome's V8 JavaScript engine. Google warned that an exploit for this vulnerability already existed in the wild and gave no further information about where it had seen abuse. Similarly, Apple released security patches to address a type-confusion vulnerability residing in Apple's Webkit browser engine. The vulnerability, tracked as CVE-2022-42856, can allow threat actors to execute arbitrary code on a targeted device if exploited via crafting malicious web content. Apple noted that the vulnerability was being exploited in the wild, but did not provide further details.

The final scene for critical vulnerability disclosures in 2022 involved the publication of proof-of-concept (POC) exploits: 1 for a Cisco IP Phone vulnerability, and 1 for a macOS vulnerability. Cisco released an advisory early in the month describing a high-severity vulnerability in Cisco's IP Phone 7800 and 8800 series. The vulnerability, tracked as CVE-2022-20968, is a stack overflow vulnerability found in all of the product versions prior to version 14.2. The Cisco Product Security Incident Response Team (PSIRT) acknowledged that POC exploit code for CVE-2022-20968 was available, and that the vulnerability "ha[d] been publicly discussed". In the same vein, Apple released a security update published to address CVE-2022-46689, also referred to as Dirty COW (dirty copy-on-write), a race-condition vulnerability affecting macOS. A few days later, software developer Zhuowei Zhang published a demo script for exploiting CVE-2022-46689, which could be used to obtain root access on macOS 13.0.1.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-4262	99	Google Chrome	Web browser		Yes
CVE-2022-27518	99	Citrix Application Delivery Controller	Network traffic controller		Yes
CVE-2022-42475	99	Fortinet FortiOS	Operating system		Yes
CVE-2022-42856	99	Apple product operating systems (such as iOS)	Operating system		Yes
CVE-2022-44698	99	Microsoft Windows and Windows Server	Operating system	Magniber, Qbot	Yes
CVE-2022-46689	99	Apple product operating systems (such as iOS)	Operating system		
CVE-2022-20968	79	Cisco IP Phone	VoIP communications		(inaccurately reported as Yes)
CVE-2022-46164	75	NodeBB	Forum development		
CVE-2022-45025	75	Markdown Preview Enhanced	Developer environment extension		

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.