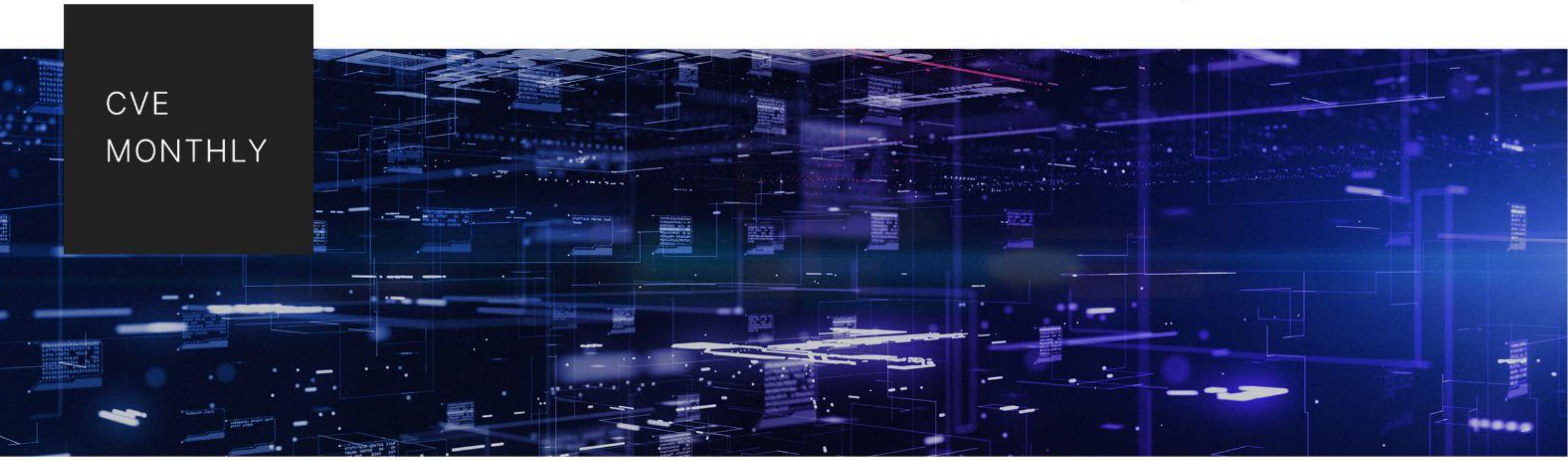

Recorded Future CVE Monthly August 2022

This report analyzes the top vulnerabilities disclosed across 8 major software vendors (Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco) from August 1 to August 31, 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 August 2022, zero-day disclosures and newly released proof-of-concept (POC) exploits were contributing factors to a high number of high-risk vulnerabilities: 11 in total. Major vendors on our prioritized list that were affected by high-risk vulnerabilities were Apple, Google, and Microsoft; other affected vendors were DrayTek, Moodle, Palo Alto Networks, Realtek, and VMWare.
- Operating systems (OSs)and web browsers were key targets in major vendor products; the categories of affected software for other vendors were more diverse.
- The "DogWalk" vulnerability, which was disclosed in 2020 but only issued a CVE identifier in August 2022, contributes to a new trend of criminals exploiting a flaw in the Microsoft Support Diagnostic Tool (MSDT) component for exploitation via a malicious document, which does not require a victim to enable macros.
- A newly trending target of threat activity is VMWare's Workspace ONE suite of products, which has now seen critical vulnerability exploitation across 2 vulnerabilities in the last 6 months.

CVE Monthly Prominent Vulnerability Disclosures

When it rains, it pours. As if the landscape was not content to simply break the dry spell of June, the number of high-risk vulnerabilities that we identified for August 2022 was over double the number from July, driven by 2 categories: disclosures of several zero-day vulnerabilities in products from major vendors like Apple, Google, and Microsoft; and releases of POC exploits for critical vulnerabilities in software from both our prioritized vendors and a diverse group of others. Unlike last month, there was a nearly equal distribution of high-risk vulnerabilities between our prioritized vendors and others. For our prioritized list, OSs and web browsers were principally affected; outside of this list, we saw a wide spread of affected components including router firmware, device management, interface controllers, and learning management software.

As is to be expected based on trends from the last several years, all of the high-risk vulnerabilities for this past month with CVSS scores were of low attack complexity. However, POC exploit code for these vulnerabilities ranged from a few lines (such as could be used against the Draytek router vulnerability CVE-2022-32548) to multi-file packages (such as were released for the Realtek eCos and Moodle vulnerabilities, CVE-2022-27255 and CVE-2020-14321, respectively).

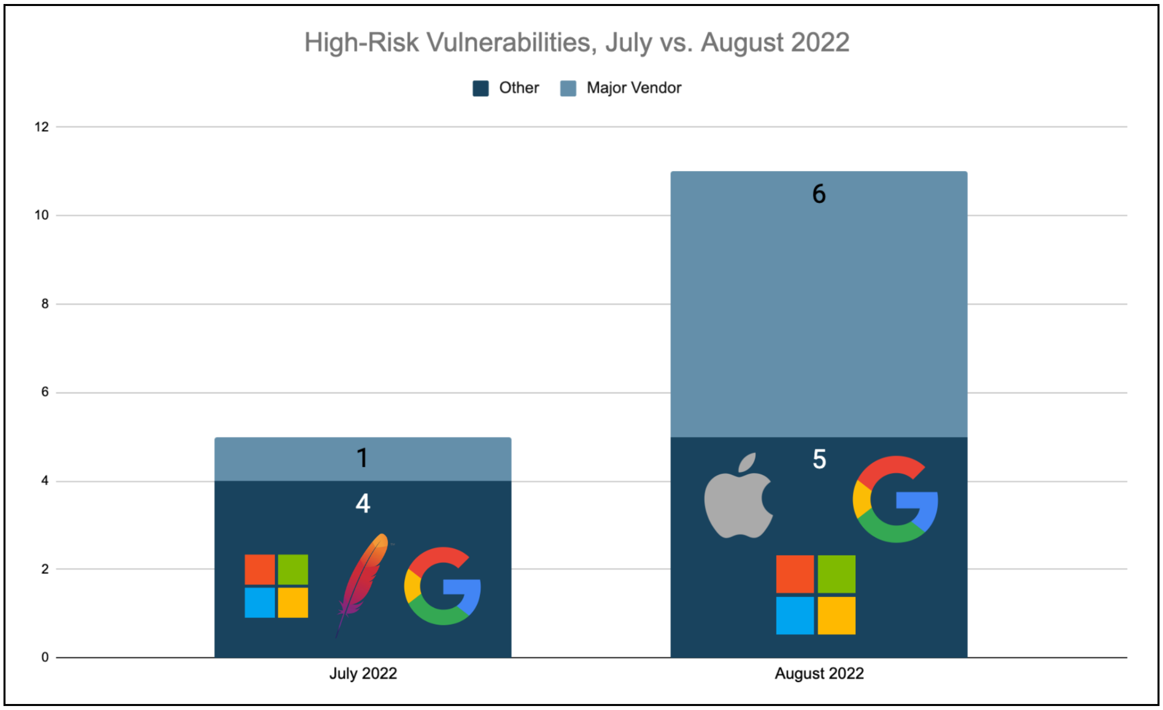

Figure 1: *Comparison of proportion of high-risk vulnerabilities between major software vendors and other vendors. In July 2022, 4 high-risk vulnerabilities affected Apache, Google, and Microsoft, while in August 2022 5 high-risk vulnerabilities affected Apple, Google, and Microsoft. There is a clear jump in high-risk vulnerabilities affecting other vendors. (Source: Recorded Future)*

The zero-day vulnerabilities this month affected Apple and Google. At least 1 other vulnerability, "DogWalk", was incorrectly identified as a zero-day since exploitation was reported after initial disclosure (with this disclosure, by security researcher Imre Rad, occurring over 2 years before a CVE identifier was assigned). However, given the trend represented by DogWalk, it is worth starting with it in a review of individual vulnerabilities.

In Microsoft's Patch Tuesday report released on August 9, 2022, Microsoft disclosed that the vulnerability dubbed DogWalk had been exploited by attackers in the wild. This vulnerability, formally tracked as CVE 2022 34713, is a remote code execution (RCE) vulnerability enabled by a path transversal weakness in the Microsoft Support Diagnostic Tool (MSDT). DogWalk affects a significant amount of Microsoft products. All Windows versions under support are affected, including the latest client and server releases: Windows 11 and Windows Server 2022.

At the time of Imre Rad's initial disclosure in January 2020, the vulnerability was not considered a significant threat to Microsoft users, and a formal patch was not provided. However, a social media post in early June 2022 brought the vulnerability back into public awareness. The post emphasized that this vulnerability is separate from the now-patched Follina (CVE 2022 30190) vulnerability disclosed by Microsoft in late May 2022, although both vulnerabilities exist in the MSDT. While Follina is an RCE vulnerability, DogWalk is a path traversal vulnerability. Follina has been exploited by multiple threat groups since its disclosure. DogWalk's exploitation confirms our suspicion of a few months ago that non-macro-related Microsoft vulnerabilities that could be exploited via malicious documents would become a trending feature of the cyber threat landscape.

In the category of actual zero-days, on August 16, 2022, Google released 11 new security fixes for newly discovered vulnerabilities, including 1 zero-day vulnerability, tracked as CVE 2022 2856, found in Google's Chromium browser. The vulnerability, reported by members of Google's Threat Analysis

Group (TAG) on July 19, 2022, is a high-severity security flaw caused by “insufficient validation of untrusted input in Intents”. The security issue affects Windows, Mac, and Linux users. While little is known about the vulnerability at this time, Google did note that an exploit exists for the vulnerability in the wild.

On August 17, 2022, Apple published security updates [1, 2] for 2 actively exploited zero-day vulnerabilities affecting the iOS, iPadOS, and macOS Monterey platforms, tracked as CVE-2022-32893 and CVE-2022-32894. CVE-2022-32893 is an out-of-bounds write vulnerability affecting the Safari WebKit that can lead to arbitrary code execution using specially crafted web content. CVE-2022-32894 is an out-of-bounds write vulnerability affecting the OS kernel that can be used to perform arbitrary code execution with the highest privileges. Both CVE-2022-32893 and CVE-2022-32894 were disclosed to Apple by an anonymous security researcher.

While they are not zero-day vulnerabilities and only 1 has seen exploitation since disclosure, 2 VMWare vulnerabilities disclosed this month are likely to become part of a trend of threat actor exploitation of vulnerabilities in VMWare’s Workspace ONE series of products. On August 2, 2022, VMWare released an advisory that included information regarding 2 critical vulnerabilities affecting its VMWare Workspace ONE Access and Identity Manager solutions: CVE-2022-31656 and CVE-2022-31659. The former vulnerability is an authentication bypass vulnerability, and the latter is a SQL injection vulnerability. A week later, on August 9, 2022, VMWare confirmed in an update to its original disclosure that POC exploit code had been published for these vulnerabilities.

VMWare Horizon has been a regularly reported target of nation-state and cybercriminal threat campaigns throughout 2022. Prior to the vulnerabilities listed above, the most recent VMWare vulnerability that has been actively exploited is CVE-2022-22954: in April 2022, Morphisec researchers disclosed the operations of the Iranian-aligned threat actor “Rocket Kitten”, which was actively exploiting CVE-2022-22954 to deploy the Core Impact penetration testing tool.

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-2022-2856	99	Google Chromium	Web browser		Yes
CVE-2022-27255	99	Realtek eCos	Interface controller		No
CVE-2022-32548	99	DrayTek Vigor	Router firmware		No
CVE-2022-32893	99	Apple Safari Webkit	Web browser		Yes
CVE-2022-32894	99	Apple iOS, iPadOS, and macOS	Operating system		Yes

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-34699	91	Microsoft Windows and Windows Server	Operating system		No
CVE-2022-31656	79	VMWare Workspace ONE Access, Identity Manager, and vRealize Automation	Device management		No
CVE-2022-31659	79	VMWare Workspace ONE Access and Identity Manager	Device management		No
CVE-2022-0028	79	Palo Alto Networks PAN-OS	Operating system		No
CVE-2022-34713	79	Microsoft Windows and Windows Server	Operating system	Quantum Software Builder	No (although inaccurately reported as such)
CVE-2020-14321	77	Moodle	Learning management system		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.