Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly June 2022

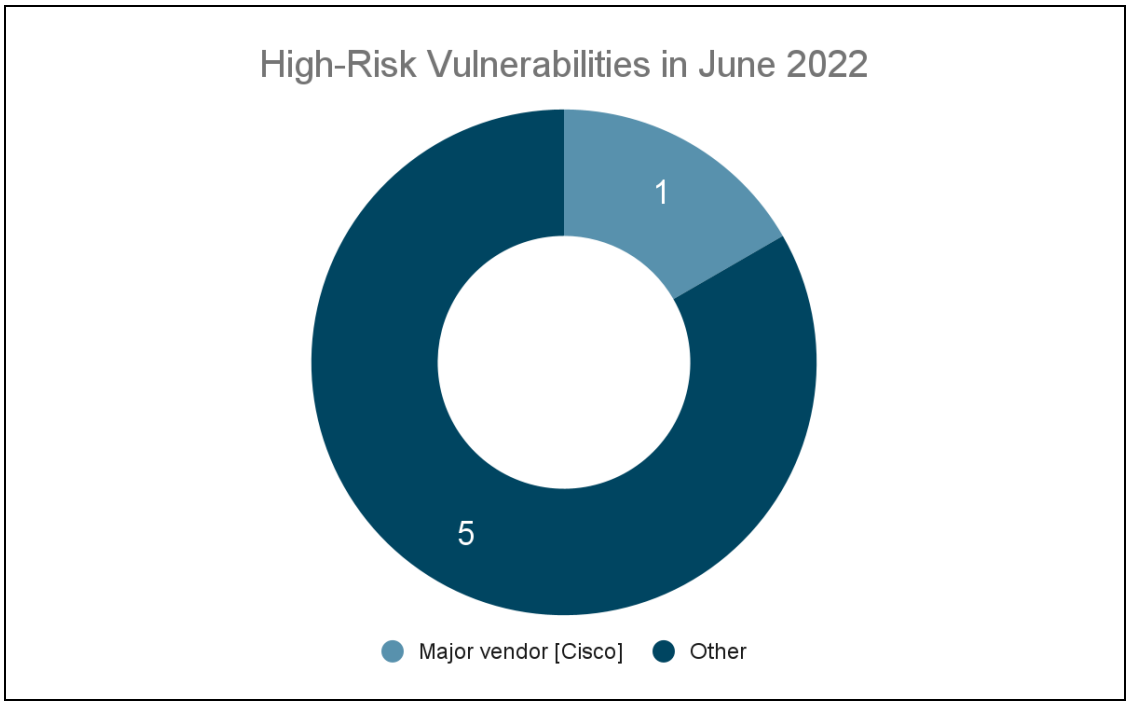
This report analyzes the top vulnerabilities disclosed across 8 major software vendors (Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco) from June 7 to July 1, 2022. This report includes the total number of vulnerabilities disclosed within the reporting period, the number of critical and zero-day vulnerabilities disclosed, the number of vulnerabilities actively exploited at the time of writing, and additional major trends and noteworthy vulnerabilities.

Key Judgments

- June 2022 was a much quieter month for newly disclosed and exploited vulnerabilities than May 2022, but this is almost certainly a temporary situation due in part to the summer holiday season for many countries.
- Out of the major vendors that we prioritize for monthly research, only Cisco disclosed a critical vulnerability that received a high risk score in the Recorded Future® Platform (CVE-2022-20829). Other high-risk vulnerabilities affected less widespread or well-known software and hardware.
- Proof-of-concept exploit code was published for 2 recently disclosed Microsoft vulnerabilities in June, lowering the bar for entry for cyber threat actors interested in exploitation.
- Hertzbleed, a vulnerability affecting all IBM processors and many AMD processors, has received widespread security research attention but no exploitation in the wild.

CVE Monthly Prominent Vulnerability Disclosures

As the old movie trope goes, "it's quiet … too quiet". The landscape for newly disclosed, high-risk vulnerabilities affecting major software vendors in June 2022 was remarkably muted. Outside of ongoing or increased exploitation of vulnerabilities identified in May like CVE-2022-30190 (Follina) in Microsoft or CVE-2022-26134 in Confluence, there have been minimal new reports of critical and exploited vulnerabilities. Outside of Cisco — which disclosed a critical (and so far unexploited) vulnerability (CVE-2022-20829) in its Adaptive Security Device Manager (ASDM) — no major vendor in our regular review disclosed a vulnerability with a high-risk score in the Recorded Future Platform. Moreover, while the Cisco vulnerability allows for remote code execution (RCE), it does also require an attacker to be previously authenticated with administrator privileges.



The few high-risk vulnerabilities aside from the one disclosed by Cisco involved less widespread or well-known products such as the router manufacturer TP-Link (CVE-2022-30075), analytics platform Grafana (CVE-2022-32275), the WordPress website builder Jupiter (CVE-2022-1654), or the Brazilian financial platform Virtua Cobranca (CVE-2021-37589). We did not see open-source reports of active exploitation in any of these cases, although for the TP-Link vulnerability, CVE-2022-30075, a proof-of-concept (POC) exploit script was published to GitHub in early June. Additionally, for TP-Link and Jupiter, our honeypot source collection saw attempts at exploitation.

This state of affairs is obviously a boon to defenders who have had to deal with panic-button vulnerabilities like Log4Shell every few months in the past year. However, it is almost certainly a temporary situation brought on by the fact that, like many industries, the cyber threat sector tends to take vacations in the summer. Security teams should be utilizing this time to shore up defenses as much as possible rather than putting their feet up and waiting for the next PrintNightmare to hit. If any previously exploited RCE vulnerabilities have not already been patched, these should be the priority, since they are certainly the priority for attackers.

Microsoft is always at the top of criminal and security research attention for vulnerability exploitation, and while nothing in the last month has been disclosed at the level of Follina, there are still a few areas where defenders of Windows systems should watch out. “DogWalk” is a vulnerability affecting Microsoft’s Diagnostic Tool (MSDT) that is similar to Follina and as of this writing has not received an official patch from Microsoft, although it has received an unofficial patch from 0patch. We have also seen POC exploits released for 2 previously disclosed Microsoft vulnerabilities: an exploit for the RCE vulnerability CVE-2022-26809 (disclosed in April), which affects recent versions of Windows and Windows Server; and an exploit for the RCE vulnerability CVE-2022-26937 (disclosed in May), which affects recent versions of Windows Server. For the former vulnerability, we’ve also seen exploitation attempts on honeypot sources.

As an honorable mention, the side-channel attack known as Hertzbleed received widespread security research attention when it was disclosed as part of a preprint paper from several US universities (the researchers will present their findings at the upcoming 31st USENIX Security Symposium, August 10 to 12, 2022). According to the researchers, Hertzbleed can be exploited without any user interaction to allow remote attackers to steal full cryptographic keys by observing variations in CPU frequency enabled by dynamic voltage and frequency scaling (DVFS), colloquially known as CPU throttling.

At this time, there are 2 known Hertzbleed-related vulnerabilities, tracked as CVE-2022-24436 (for Intel processors) and CVE-2022-22823 (for AMD processors). Both Intel and AMD have confirmed that Hertzbleed affects all or many of their processors, respectively. Moreover, the researchers who disclosed Hertzbleed have publicly released the source code for all of the experiments outlined in their paper. All that said, we have not yet seen news of in-the-wild exploitation, nor have we seen any references to threat actors advertising or soliciting POC exploit code for Hertzbleed on any of the dark web or underground forum sources in Recorded Future’s datasets.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-30075	99	TP-Link Router AX50	Router firmware		No
CVE-2022-32275	93	Grafana	Analytics platform		No
CVE-2022-1654	83	Artbees Jupiter for WordPress	Website builder		No
CVE-2021-37589	82	Virtua Cobranca	Corporate finance management		No
CVE-2022-20829	80	Cisco Adaptive Security Device Manager	Security appliance manager		No
CVE-2022-31626	79	PHP	Scripting language		No
CVE-2022-30075	99	TP-Link Router AX50	Router firmware		No
CVE-2022-32275	93	Grafana	Analytics 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.