Recorded Future®

CVE
MONTHLY

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 July 1 to July 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

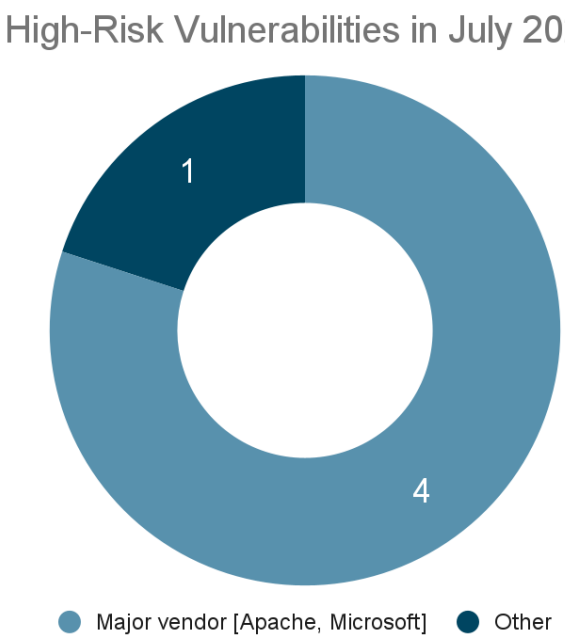
- July 2022 was a return to form for vulnerability exploitation after a light June, with cyberattacks against high-risk vulnerabilities affecting Apache, Google, and Microsoft.
- Spyware was the common thread across at least 2 cases of vulnerability exploitation, one involving an Austria-based threat group exploiting a flaw in Microsoft Windows and another an Israeli-based threat group exploiting a flaw in Google Chrome.
- The prominent vulnerability Follina (CVE-2022-30190) continued to see exploitation by new threat groups, including a group that exploited it to distribute the Rozena backdoor..

CVE Monthly Prominent Vulnerability Disclosures

As we assessed in our last report, the calm of June 2022 was unlikely to persist through to July. Security researchers found exploitation of zero-day vulnerabilities affecting Microsoft and Google, in both cases to distribute spyware, demonstrating the often close link between top-of-the-line spyware developers and zero-day exploitation. A data analytics tool from Apache (Apache Spark) also saw publication of a proof-of-concept (POC) exploit and exploitation within days after initial disclosure. (As this vulnerability has low attack complexity, this speed is not surprising.)

On July 4, 2022, Google disclosed an actively exploited zero-day vulnerability, CVE-2022-2294, which affects Google Chrome. While the company did not disclose details about attacks involving this flaw, it was not long before exploitation was reported by others. Avast threat researchers (who had originally informed Google about the vulnerability) released a report on July 21, 2022, about a campaign in which Israeli spyware vendor Candiru exploited CVE-2022-2294 to deploy DevilsTongue spyware.

Spyware was associated with another zero-day vulnerability, this time for Microsoft. On July 12, 2022, Microsoft disclosed a zero-day vulnerability, CVE-2022-22047, that affects current versions of Windows and Windows Server. This vulnerability was exploited by the Austria-based mercenary threat group KNOTWEED to distribute its Subzero spyware. A second vulnerability, CVE-2022-30216, also affects current versions of Windows and Windows Server and has a very high CVSS score due to allowing remote code execution (RCE), but we have not yet seen exploitation attempts.



Aside from Microsoft and Google, the only other major vendor to see a high-risk vulnerability was Apache. In mid-July 2022, security researcher Kostya Kortchinsky of Databricks disclosed a vulnerability in Apache Spark (CVE-2022-33891) that would allow an attacker to use an arbitrary username if access control lists (ACL) were enabled to perform remote code execution. Within 3 days after the disclosure from Apache, a proof-of-concept exploit was published to GitHub, and within 2 days after that, Recorded Future identified attempted exploitation via our honeypot source.

If we could have predicted any vulnerability to see high-profile exploitation after initial disclosure, it would have been Follina. Sure enough, on July 6, 2022, Fortinet researchers released an analytic report on a phishing campaign using the recently discovered Follina vulnerability (CVE-2022-30190) to distribute the Rozena backdoor, a malware that allows attackers to completely take over Windows systems. Fortinet researchers observed adversaries using Rozena to inject a remote shell connection back to the attacker's machine.

The 1 vulnerability that we identified as high risk for July, but which did not affect a major vendor, was CVE-2022-34265, which affects the Python web framework Django. On July 4, 2022, Django released patches to fix a high-severity potential SQL injection vulnerability (CVE-2022-34265) in 2 of its functions.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2022-33891	99	Apache Spark	Data analytics tool		No
CVE-2022-22047	99	Microsoft Windows and Windows Server	Operating system	Subzero	Yes
CVE-2022-2294	89	Google Chrome	Web browser	DevilsTongue	Yes
CVE-2022-30216	79	Microsoft Windows and Windows Server	Operating system		Yes
CVE-2022-34265	79	Django	Web framework		No
CVE-2022-33891	99	Apache Spark	Data analytics tool		No
CVE-2022-22047	99	Microsoft Windows and Windows Server	Operating system	Subzero	Yes
CVE-2022-2294	89	Google Chrome	Web browser	DevilsTongue	Yes

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.