

Exploitation of 55 Zero-Day Vulnerabilities Came to Light in 2022: Mandiant



Google-owned Mandiant has conducted an analysis of the zero-day vulnerabilities disclosed in 2022 and found that over a dozen of them were used in attacks believed to have been carried out by cyberespionage groups.

The cybersecurity community cannot reach an agreement on the definition of zero-day vulnerability. Some define as zero-day any vulnerability whose details are made public before a patch is released, while others only assign a zero-day classification to flaws that were actually exploited in attacks before a fix was made available.

Mandiant noted that only vulnerabilities that were exploited in the wild before a patch was released were included in its zero-day analysis.

According to Mandiant, 55 zero-day vulnerabilities came to

light last year. While this is a significant drop from the 81 discovered in 2021, it's still more than in any other previous year.

Many of the zero-days found last year were not publicly attributed to a known threat actor. Of the ones that were attributed, 13 were linked to cyberespionage groups, including seven believed to have been exploited by Chinese state-sponsored groups.

Chinese hackers targeted vulnerabilities such as CVE-2022-30190 (the Windows flaw known as Follina), and CVE-2022-42475 and CVE-2022-41328 (Fortinet product vulnerabilities).

Two of the zero-days attributed to state-sponsored threat actors were linked to North Korea and two were tied to Russia. Three vulnerabilities were exploited by commercial spyware vendors such as Candiru and Variston. One flaw was seen being exploited by both China and Russia, and spyware vendors as well.

Four of the zero-days spotted in 2022 were likely exploited by financially motivated threat actors, including CVE-2022-29499 (by Lorenz ransomware), and CVE-2022-41091 and CVE-2022-44698 (by Magniber ransomware).

Of the 55 zero-days that emerged in 2022, 18 impacted Microsoft products, 10 impacted Google products, and 9 were found in Apple products. Other affected vendors included Fortinet, Mozilla, Sophos, Trend Micro, Zimbra, Adobe, Atlassian, Cisco, Mitel, SolarWinds, Zoho, QNAP, and Citrix.

As for product types, 19 flaws impacted desktop operating systems, followed by browsers (11), security, IT and network management products (10), and mobile operating systems (6).

"Almost all 2022 zero-day vulnerabilities (53) were exploited for the purpose of achieving either (primarily remote) code

execution or gaining elevated privileges, both of which are consistent with most threat actor objectives,” Mandiant noted.

Additional details, including information on why temporary workarounds can cause defender fatigue, are available in Mandiant’s full report.

Related: Dozens of Exploited Vulnerabilities Missing From CISA ‘Must Patch’ List

Related: 557 CVEs Added to CISA’s Known Exploited Vulnerabilities Catalog in 2022

<https://www.securityweek.com/exploitation-of-55-zero-day-vulnerabilities-came-to-light-in-2022-mandiant/>