Security Enrichment Report

Generated: 2025-09-07T06:04:18.283856

CVE-2024-7264 — Score 58.0

A vulnerability in curl versions 7.32.0 through 8.9.0, discovered on July 30, 2024, could lead to a crash or heap content exposure when exploited, particularly when CURLINFO_CERTINFO is used. The issue has been addressed in curl version 8.9.1.

Citations:

https://www.cisa.gov/known-exploited-vulnerabilities-catalog?_gl=1%2A4l6zte%2A_ga%2ANzM5MTk2MTAxLjE2
https://www.rapid7.com/blog/post/2024/11/15/etr-zero-day-exploitation-targeting-palo-alto-networks-f
https://nvd.nist.gov/vuln/detail/cve-2024-7971

CVE-2023-12345 — Score 50.0

CVE-2023-12345 is a known vulnerability that has been actively exploited in incidents. These incidents involved spear-phishing tactics and affected public-facing applications and internal systems.

Citations:

https://feedly.com/cve/CVE-2023-12345
https://v0.app/t/pQy3cSSN9mo
https://socradar.io/labs/app/cve-radar/cve-2023-12345

CVE-2022-26134 — Score 43.0

CVE-2022-26134 is a critical, unauthenticated remote code execution (RCE) vulnerability primarily affecting Atlassian Confluence Server and Confluence Data Center. This vulnerability allows a remote, unauthenticated attacker to bypass Servlet Filters used by first and third-party apps, leading to RCE. All supported and likely all versions of Confluence Server and Data Center are affected. Fixes have been deployed to Atlassian Cloud sites. Atlassian published a security advisory on June 2, 2022, detailing this issue.

Citations:

https://www.oracle.com/security-alerts/cpujul2022.html
https://confluence.atlassian.com/security/multiple-products-security-advisory-cve-2022-26136-cve-202
https://www.rapid7.com/blog/post/2022/06/02/active-exploitation-of-confluence-cve-2022-26134/

CVE-2020-9999 — Score 25.5

An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability.

Citations:

https://access.redhat.com/security/cve/cve-2020-9999
https://www.cve.org/CVERecord?id=CVE-2020-9999
https://nvd.nist.gov/vuln/detail/CVE-2020-9999/change-record?changeRecordedOn=03/11/2021T11:28:00.73