Vulnerabilities overview.

In March, 2023, 2 vulnerabilities had been publicly released.

CVE-2050-002.

The vulnerability has been published on March 17, 2023. Its description is:

The Image Hover Effects Css3 WordPress plugin through 4.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).

The vulnerability's CVSS score is not provided.

Associated reports.

No entities found.

Recommendations.

No entities found.

CVE-2050-001.

The vulnerability has been published on March 17, 2023. Its description is

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution.

Its CVSS score is not provided.

Associated reports.

No entities found.

Recommendations.

No entities found.