Fortinet Rolls Out Critical Security Patches for FortiClient Linux Vulnerability

Date: 11th April 2024 | Severity: High

Summary

Fortinet has released patches to address a critical security flaw impacting FortiClient Linux that could be exploited to achieve arbitrary code execution.

Attack Vectors

An Improper Control of Generation of Code (‘Code Injection’) vulnerability [CWE-94] in FortiClient Linux may allow an unauthenticated attacker to execute arbitrary code via tricking a FortiClient Linux user into visiting a malicious website.

Vulnerability tracked as CVE-2023-45590 and carries a CVSS score of 9.4 out of a maximum of 10.

The product constructs all or part of a code segment using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Recommendation

While there is no evidence of any of the flaws being exploited in the wild, it’s recommended that users keep their systems up to date to mitigate potential threats.

Version	Affected	Solution
FortiClient Linux 7.2	7.2.0	Upgrade to 7.2.1 or above
FortiClient Linux 7.0	7.0.6 through 7.0.10	Upgrade to 7.0.11 or above
FortiClient Linux 7.0	7.0.3 through 7.0.4	Upgrade to 7.0.11 or above

Reference Links

- https://www.fortiguard.com/psirt/FG-IR-23-087
- https://www.cvedetails.com/cve/CVE-2023-45590/?q=CVE-2023-45590
- https://thehackernews.com/2024/04/fortinet-has-released-patches-to.html