

Clickjacking Vulnerability (CVE-2021-35237)

Summary

A missing HTTP header (X-Frame-Options) in Kiwi Syslog Server has left customers vulnerable to click jacking. Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage. The attacker essentially hijacks the user activity intended for the original server and sends them to the other server. This is an attack on both the user and the server.

Affected Products

- Kiwi Syslog Server 9.7.2 and earlier

Fixed Software Release

- [Kiwi Syslog Server 9.8](#)

Advisory Details

Severity

5.0 Medium

Advisory ID

[CVE-2021-35237](#)

First Published

10/19/2021

Fixed Version

Kiwi Syslog Server 9.8

CVSS Score

[CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L](#)