Unquoted Path Vulnerability - SMB Login (CVE-2021-35231)

Summary

As a result of an unquoted service path vulnerability present in the Kiwi Syslog Server Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. Example vulnerable path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Kiwi Syslog Server\Parameters\Application

Affected Products

- Kiwi Syslog Server 9.7.2 and earlier

Fixed Software Release

- Kiwi Syslog Server 9.8

Acknowledgments

- David Rickard
- Danijel Grah

Advisory Details

Severity

6.7 Medium

Advisory ID

CVE-2021-35231

First Published

10/19/2021

Fixed Version

Kiwi Syslog Server 9.8

CVSS Score

3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H