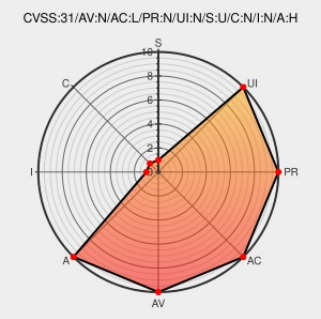
CVE-2021-3166

Published on: 01/17/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:53 PM UTC

CVE-2021-3166

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dsl-n14u B1 from Asus contain the following vulnerability:

An issue was discovered on ASUS DSL-N14U-B1 1.1.2.3_805 devices. An attacker can upload arbitrary file content as a firmware update when the filename Settings_DSL-N14U-B1.trx is used. Once this file is loaded, shutdown measures on a wide range of services are triggered as if it were a real update, resulting in a persistent outage of those services.

CVE-2021-3166 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
kaisersource.github.io/2021-01-17-dsl-n14u.md at main ·	Exploit, Third Party Advisory	MISC github.com/kaisersource/kaisersource.github.io/blob/main/_posts/2021-

kaisersource/kaisersource.github.io · GitHub	github.com text/html	01-17-dsl-n14u.md
Asus DSL-N14U DoS	Exploit Third Party Advisory kaisersource.github.io text/html	MISC kaisersource.github.io/dsl-n14u

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Mastering CVE-2021-3166

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Dsl-n14u B1	-	All	All	All
Hardware	Asus	Dsl-n14u B1	-	All	All	All
Hardware	Asus	Dsl-n14u B1	-	All	All	All
Operating System	Asus	Dsl-n14u B1 Firmware	1.1.2.3_805	All	All	All
Operating System	Asus	Dsl-n14u B1 Firmware	1.1.2.3_805	All	All	All

cpe:2.3:h:asus:dsl-n14u_b1:-:*:*:*:*:*:*:*:

cpe:2.3:h:asus:dsl-n14u_b1:-:*:*:*:*:*:*:*:

cpe:2.3:h:asus:dsl-n14u_b1:-:*:*:*:*:*:*:*:

cpe:2.3:o:asus:dsl-n14u_b1_firmware:1.1.2.3_805:*:*:*:*:*:*:*:

cpe:2.3:o:asus:dsl-n14u_b1_firmware:1.1.2.3_805:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report