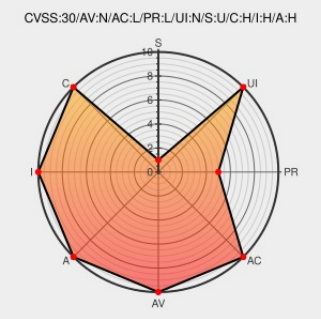
CVE-2018-11345

Published on: 05/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11345

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



Certain versions of As6202t from Asustor contain the following vulnerability:

An unrestricted file upload vulnerability in upload.cgi in ASUSTOR AS6202T ADM 3.1.0.RFQ3 allows attackers to upload supplied data via the POST parameter filename. This can be used to place attacker controlled code on the file system that can then be executed. Further, the filename parameter is vulnerable to path traversal and allows the attacker to place the file anywhere on the system.

CVE-2018-11345 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: ASUSTOR ADM 3.1.0.RFQ3 and below vulnerabilities	Mailing List Third Party Advisory	FULLDISC 20180429 ASUSTOR ADM 3.1.0.RFQ3 and below vulnerabilities

	seclists.org text/html	
No Description Provided	Exploit Third Party Advisory www.purehacking.com text/html	MISC www.purehacking.com/blog/matthew-fulton/back-to-the-future-asustor-web-exploitation
GitHub - mefulton/asustorexploit	Exploit Third Party Advisory github.com text/html	MISC github.com/mefulton/asustorexploit

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asustor	As6202t	-	All	All	All
Hardware	Asustor	As6202t	-	All	All	All
Operating System	Asustor	As6202t Firmware	All	All	All	All

cpe:2.3:h:asustor:as6202t:-:*:*:*:*:*:*:*:

cpe:2.3:h:asustor:as6202t:-:*:*:*:*:*:*:*:

cpe:2.3:o:asustor:as6202t_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→