



# CVE-2017-15653

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2017-15653
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-01-31 20:29:00 UTC
<b>Updated</b>	2018-02-27 18:31:00 UTC
<b>Description</b>	Improper administrator IP validation after his login in the HTTPd server in all current versions (<= 3.0.0.4.380.7743) of Asus

## Risk And Classification

**Problem Types:** CWE-613

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asus	Asuswrt	All	All	All	All

## References

Reference	Source	Link	Tags
ASUSWRT 3.0.0.4.382.18495 Session Hijacking / Information Disclosure ~ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>	Third Pa
Full Disclosure: Multiple vulnerabilities in all versions of ASUS routers	FULLDISC	<a href="http://seclists.org">seclists.org</a>	Mailing L
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered 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](#)**