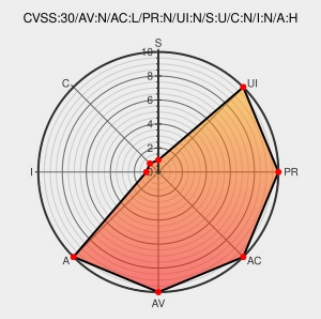
CVE-2018-16789

Published on: 03/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16789

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



Certain versions of Shellinabox from Shellinabox Project contain the following vulnerability:

libhttp/url.c in shellinabox through 2.20 has an implementation flaw in the HTTP request parsing logic. By sending a crafted multipart/form-data HTTP request, an attacker could exploit this to force shellinaboxd into an infinite loop, exhausting available CPU resources and taking the service down.

CVE-2018-16789 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: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Full Disclosure: CVE-2018-16789: denial of service in shellinabox	Exploit Mailing List Patch	MISC seclists.org/fulldisclosure/2018/Oct/50

	Third Party Advisory seclists.org text/html	
Shell In A Box 2.2.0 Denial Of Service ≈ Packet Storm	Exploit Patch Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/149978/Shell-In-A-Box-2.2.0-Denial-Of-Service.html
Rolling code for version 2.21 · shellinabox/shellinabox@4f0ecc3 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/shellinabox/shellinabox/commit/4f0ecc31ac6f985e0dd3f5a52cbfc0e
Google Code Archive - Long-term storage for Google Code Project Hosting.	Third Party Advisory code.google.com text/html	CONFIRM code.google.com/archive/p/shellinabox/issues

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
Application	Shellinabox Project	Shellinabox	All	All	All	All

cpe:2.3:a:shellinabox_project:shellinabox:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→