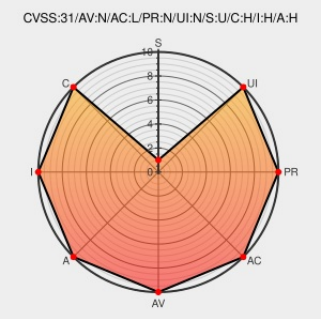
CVE-2018-18439

Published on: 11/20/2018 12:00:00 AM UTC

Last Modified on: 01/23/2023 06:39:00 PM UTC

CVE-2018-18439

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



Certain versions of Das U-boot from Denx contain the following vulnerability:

DENX U-Boot through 2018.09-rc1 has a remotely exploitable buffer overflow via a malicious TFTP server because TFTP traffic is mishandled. Also, local exploitation can occur via a crafted kernel image.

CVE-2018-18439 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
oss-security - CVE-2018-18439, CVE-2018-18440 - U-Boot verified boot bypass vulnerabilities	Exploit, Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20181102 CVE-2018-18439, CVE-2018-18440 - U-Boot verified boot bypass vulnerabilities

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	Denx	Das U-boot	-	All	All	All
Hardware	Denx	Das U-boot	-	All	All	All
Operating System	Denx	Das U-boot Firmware	All	All	All	All
Application	Denx	U-boot	All	All	All	All
Application	Denx	U-boot	2018.09	rc1	All	All

cpe:2.3:h:denx:das_u-boot:-:*:*:*:*:*:*:*:

cpe:2.3:h:denx:das_u-boot:-:*:*:*:*:*:*:*:

cpe:2.3:o:denx:das_u-boot_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:a:denx:u-boot:*:*:*:*:*:*:*:*:

cpe:2.3:a:denx:u-boot:2018.09:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→