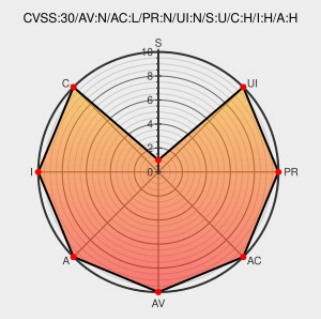
CVE-2018-14060

Published on: 07/14/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-14060

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



Certain versions of Xiaomi R3d from Mi contain the following vulnerability:

OS command injection in the AP mode settings feature in /cgi-bin/luci /api/misystem/set_router_wifiap on Xiaomi R3D before 2.26.4 devices allows an attacker to execute any command via crafted JSON data.

CVE-2018-14060 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
国家信息安全漏洞共享平台	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.cnvd.org.cn/flaw/show/CNVD-2018-04520

router/CNVD-2018-04520.py at master · cc-crack/router · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/cc-crack/router/blob/master/CNVD-2018-04520.py

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mi	Xiaomi R3d	-	All	All	All
Hardware	Mi	Xiaomi R3d	-	All	All	All
Operating System	Mi	Xiaomi R3d Firmware	All	All	All	All
Operating System	Mi	Xiaomi R3d Firmware	All	All	All	All

cpe:2.3:h:mi:xiaomi_r3d:-:*:*:*:*:*:*:*:

cpe:2.3:h:mi:xiaomi_r3d:-:*:*:*:*:*:*:*:

cpe:2.3:o:mi:xiaomi_r3d_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:mi:xiaomi_r3d_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→