



CVE-2018-16307

Published on: 09/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

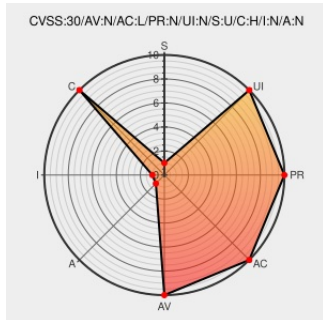
CVE-2018-16307

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Xiaomi Miwifi Xiaomi 55dd](#) from [Mi](#) contain the following vulnerability:

An "Out-of-band resource load" issue was discovered on Xiaomi MIWiFi Xiaomi_55DD Version 2.8.50 devices. It is possible to induce the application to retrieve the contents of an arbitrary external URL and return those contents in its own response. If a domain name (containing a random string) is used in the HTTP Host header, the application performs an HTTP request to the specified domain. The response from that request is then included in the application's own response.

CVE-2018-16307 has been assigned by [M](#) 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	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
MIWIFI: Xiaomi_55DD 2.8.50 Out Of Band	Exploit	MISC packetstormsecurity.com/files/140106/MIWIFI

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 📺🔗	Mi	Xiaomi Miwifi Xiaomi 55dd	-	All	All	All
Hardware 📺🔗	Mi	Xiaomi Miwifi Xiaomi 55dd	-	All	All	All
Operating System	Mi	Xiaomi Miwifi Xiaomi 55dd Firmware	2.8.50	All	All	All
Operating System	Mi	Xiaomi Miwifi Xiaomi 55dd Firmware	2.8.50	All	All	All
cpe:2.3:h:mi:xiaomi_miwifi_xiaomi_55dd:-:*:*:*:*:*:						
cpe:2.3:h:mi:xiaomi_miwifi_xiaomi_55dd:-:*:*:*:*:*:						
cpe:2.3:o:mi:xiaomi_miwifi_xiaomi_55dd_firmware:2.8.50:*:*:*:*:*:						
cpe:2.3:o:mi:xiaomi_miwifi_xiaomi_55dd_firmware:2.8.50:*:*:*:*:*:						

Next ID→