



CVE-2017-12223

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

Summary

CVE	CVE-2017-12223
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-07 21:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the ROM Monitor (ROMMON) code of Cisco IR800 Integrated Services Router Software could allow an un

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Ir800 Integrated Services Router	-	All	All	All
Hardware	Cisco	Ir800 Integrated Services Router	-	All	All	All
Operating System	Cisco	Ir800 Integrated Services Router Firmware	-	All	All	All
Operating System	Cisco	Ir800 Integrated Services Router Firmware	-	All	All	All

References

Reference	Source	Label
Cisco IR800 Integrated Services Routers Input Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTrack	v
Cisco IR800 Integrated Services Router ROM Monitor Input Validation Vulnerability	CONFIRM	t
Cisco IR800 Integrated Services Router Software CVE-2017-12223 Local Code Execution Vulnerability	BID	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)