



CVE-2016-8731

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

Summary

CVE	CVE-2016-8731
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-21 19:29:00 UTC
Updated	2022-12-14 13:40:00 UTC
Description	Hard-coded FTP credentials (r:r) are included in the Foscam C1 running firmware 1.9.1.12. Knowledge of these credentials

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Foscam	C1 Webcam	-	All	All	All
Hardware	Foscam	C1 Webcam	-	All	All	All
Operating System	Foscam	C1 Webcam Firmware	1.9.1.12	All	All	All
Operating System	Foscam	C1 Webcam Firmware	1.9.1.12	All	All	All

References

Reference	Source	Link
Foscam C1 Webcam CVE-2016-8731 Hard Coded Credentials Authentication Bypass Vulnerability	BID	www.securityfocus.com
TALOS-2016-0245 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	www.talosintelligence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)