

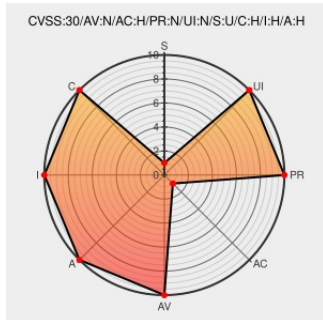


CVE-2017-2857

Published on: 09/17/2018 12:00:00 AM UTC

Last Modified on: 06/07/2022 05:26:00 PM UTC

CVE-2017-2857

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **C1** from **Foscam** contain the following vulnerability:

An exploitable buffer overflow vulnerability exists in the DDNS client used by the Foscam C1 Indoor HD Camera running application firmware 2.52.2.43. On devices with DDNS enabled, an attacker who is able to intercept HTTP connections will be able to fully compromise the device by creating a rogue HTTP server.

CVE-2017-2857 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foscam** - **Foscam Indoor IP Camera C1 Series** version **System Firmware Version: 1.9.3.18, Application Firmware Version: 2.52.2.43, Plug-In Version: 3.3.0.26**

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
TALOS-2017-0360 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third-Party Advisory	MISC www.talosintelligence.com/vulnerability-reports/TALOS-2017-0360

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Foscam	C1	-	All	All	All
Hardware	Foscam	C1	-	All	All	All
Operating System	Foscam	C1 Firmware	2.52.2.43	All	All	All
Operating System	Foscam	C1 Firmware	2.52.2.43	All	All	All
cpe:2.3:h:foscam:c1:-:*:*:*:*:*:						
cpe:2.3:h:foscam:c1:-:*:*:*:*:*:						
cpe:2.3:o:foscam:c1_firmware:2.52.2.43:*:*:*:*:*:						
cpe:2.3:o:foscam:c1_firmware:2.52.2.43:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Next ID→