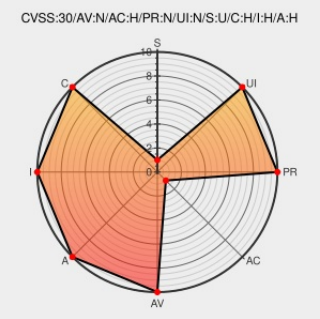
CVE-2017-2855

Published on: 09/19/2018 12:00:00 AM UTC

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

CVE-2017-2855

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-2017-2855 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Foscam** - **Foscam C1 Indoor HD Camera** version **Foscam Indoor IP Camera C1 Series,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-2017-0358 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit, Third Party Advisory	MISC talosintelligence.com/vulnerability_reports/TALOS-

Comprehensive Threat Intelligence

Third Party Advisory
talosintelligence.com
text/html
talosintelligence.com/vulnerability_reports/TALOS-2017-0358

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

← Previous ID

Next ID→