



CVE-2021-1596

Published on: 07/08/2021 12:00:00 AM UTC

Last Modified on: 07/13/2021 01:44:00 PM UTC

CVE-2021-1596 - advisory for cisco-sa-ipcamera-lldp-mem-wGqundTq

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

CVSS:31/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Video Surveillance 7070](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of

certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).

CVE-2021-1596 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **MEDIUM** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco Video Surveillance 7000 Series IP Cameras** version n/a

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

ADJACENT_NETWORK

LOW

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Cisco Video Surveillance 7000 Series IP Cameras Link Layer Discovery Protocol Memory Leak Vulnerabilities

tools.cisco.com

text/html

CISCO 20210707 Cisco Video Surveillance 7000 Series IP Cameras Link Layer Discovery Protocol Memory Leak Vulnerabilities

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	Cisco	Video Surveillance 7070	-	All	All	All
Operating System	Cisco	Video Surveillance 7070 Firmware	All	All	All	All
Hardware	Cisco	Video Surveillance 7530pd	-	All	All	All
Operating System	Cisco	Video Surveillance 7530pd Firmware	All	All	All	All

cpe:2.3:h:cisco:video_surveillance_7070:-:*****:

cpe:2.3:o:cisco:video_surveillance_7070_firmware:*****:

cpe:2.3:h:cisco:video_surveillance_7530pd:-:*****:

cpe:2.3:o:cisco:video_surveillance_7530pd_firmware:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-1596 : Multiple vulnerabilities in the Link Layer Discovery Protocol LLDP implementation for Cisco Video... twitter.com/i/web/status/1...	2021-07-08 18:46:09
/r/netcve	CVE-2021-1596	2021-07-08 19:41:12

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

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](#).

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