

CVE-2019-3929

Crestron Multiple Products Command Injection Vulnerability

Exigent

CISA KEV since Apr 15, 2022

Actively exploited

Public exploit module (Metasploit)

The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WiPG-1000P firmware 2.3.0.10, Barco wePresent WiPG-1600W before firmware 2.4.1.19, Extron ShareLink 200/250 firmware 2.0.3.4, Teq AV IT WIPS710 firmware 1.1.0.7, SHARP PN-L703WA firmware 1.4.2.3, Optoma WPS-Pro firmware 1.0.0.5, Blackbox HD WPS firmware 1.0.0.5, InFocus LiteShow3 firmware 1.0.16, and InFocus LiteShow4 2.0.0.7 are vulnerable to command injection via the file_transfer.cgi HTTP endpoint. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.

EVRs

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.990

99.93rd percentile · FIRST

CISA DEADLINE

May 6, 2022

KEV since 2022 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.990 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 16 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
am-100 firmware	1.6.0.2	no fixed version listed	NVD
am-101 firmware	2.7.0.2	no fixed version listed	NVD
wepresent wipg-1000p firmware	2.3.0.10	no fixed version listed	NVD
wepresent wipg-1600w firmware	< 2.4.1.19	2.4.1.19	NVD
sharelink 200 firmware	2.0.3.4	no fixed version listed	NVD
sharelink 250 firmware	2.0.3.4	no fixed version listed	NVD
wips710 firmware	1.1.0.7	no fixed version listed	NVD
pn-l703wa firmware	1.4.2.3	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-m297-v8rg-x5fh	NVD	nvd.nist.gov/vuln/detail/CVE-2019-3929
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-13536
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-3929		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.