CVE-2019-3929

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-3929
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-30 21:29:00 UTC
Updated	2020-10-16 18:09:00 UTC
Description	The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WiPG-1000P firmware 2.3.0.1

Risk And Classification

EPSS: 0.942530000 probability, percentile 0.999310000 (date 2026-04-01)

CISA KEV: Listed on 2022-04-15; due 2022-05-06; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Crestron
Product	Multiple Products
Name	Crestron Multiple Products Command Injection Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-3929

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Barco	Wepresent Wipg-1000p	-	All	All	All
Hardware	Barco	Wepresent Wipg-1000p	-	All	All	All
Operating System	Barco	Wepresent Wipg-1000p Firmware	2.3.0.10	All	All	All
Operating System	Barco	Wepresent Wipg-1000p Firmware	2.3.0.10	All	All	All
Hardware	Barco	Wepresent Wipg-1600w	-	All	All	All
Hardware	Barco	Wepresent Wipg-1600w	-	All	All	All
Operating System	Barco	Wepresent Wipg-1600w Firmware	All	All	All	All
Operating System	Barco	Wepresent Wipg-1600w Firmware	All	All	All	All

Hardware	Blackbox	Hd Wireless Presentation System	-	All	All	All
Hardware	Blackbox	Hd Wireless Presentation System	-	All	All	All
Operating System	Blackbox	Hd Wireless Presentation System Firmware	1.0.0.5	All	All	All
Operating System	Blackbox	Hd Wireless Presentation System Firmware	1.0.0.5	All	All	All
Hardware	Crestron	Am-100	-	All	All	All
Hardware	Crestron	Am-100	-	All	All	All
Operating System	Crestron	Am-100 Firmware	1.6.0.2	All	All	All
Operating System	Crestron	Am-100 Firmware	1.6.0.2	All	All	All
Hardware	Crestron	Am-101	-	All	All	All
Hardware	Crestron	Am-101	-	All	All	All
Operating System	Crestron	Am-101 Firmware	2.7.0.2	All	All	All
Operating System	Crestron	Am-101 Firmware	2.7.0.2	All	All	All
Hardware	Extron	Sharelink 200	-	All	All	All
Hardware	Extron	Sharelink 200	-	All	All	All
Operating System	Extron	Sharelink 200 Firmware	2.0.3.4	All	All	All
Operating System	Extron	Sharelink 200 Firmware	2.0.3.4	All	All	All
Hardware	Extron	Sharelink 250	-	All	All	All
Hardware	Extron	Sharelink 250	-	All	All	All
Operating System	Extron	Sharelink 250 Firmware	2.0.3.4	All	All	All
Operating System	Extron	Sharelink 250 Firmware	2.0.3.4	All	All	All
Hardware	Infocus	Liteshow3	-	All	All	All
Hardware	Infocus	Liteshow3	-	All	All	All
Operating System	Infocus	Liteshow3 Firmware	1.0.16	All	All	All
Operating System	Infocus	Liteshow3 Firmware	1.0.16	All	All	All
Hardware	Infocus	Liteshow4	-	All	All	All
Hardware	Infocus	Liteshow4	-	All	All	All
Operating System	Infocus	Liteshow4 Firmware	2.0.0.7	All	All	All
Operating System	Infocus	Liteshow4 Firmware	2.0.0.7	All	All	All
Hardware	Optoma	Wps-pro	-	All	All	All
Hardware	Optoma	Wps-pro	-	All	All	All
Operating System	Optoma	Wps-pro Firmware	1.0.0.5	All	All	All
Operating System	Optoma	Wps-pro Firmware	1.0.0.5	All	All	All
Hardware	Sharp	Pn-l703wa	-	All	All	All
Hardware	Sharp	Pn-l703wa	-	All	All	All
Operating System	Sharp	Pn-l703wa Firmware	1.4.2.3	All	All	All

Operating System	Sharp	Pn-l703wa Firmware	1.4.2.3	All	All	All
Hardware	Teqavit	Wips710	-	All	All	All
Hardware	Teqavit	Wips710	-	All	All	All
Operating System	Teqavit	Wips710 Firmware	1.1.0.7	All	All	All
Operating System	Teqavit	Wips710 Firmware	1.1.0.7	All	All	All

References

Reference
Crestron AM/Barco wePresent WiPG/Extron ShareLink/Teq AV IT/SHARP PN-L703WA/Optoma WPS-Pro/Blackbox HD WPS/InFocus LiteSh
OEM Presentation Platform Vulnerabilities - Research Advisory | Tenable®
Barco WePresent file_transfer.cgi Command Injection ≈ Packet Storm
Barco/AWIND OEM Presentation Platform Unauthenticated Remote Command Injection ≈ Packet Storm
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.