Horner Automation Cscape and XL4, XL7 PLC Weak password requirements

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6284
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 16:17:07 UTC
Updated	2026-04-20 16:16:50 UTC
Description	An attacker with network access to the PLC is able to brute force discover passwords to gain unauthorized access to syster

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000110000 probability, percentile 0.014030000 (date 2026-04-21)

Problem Types: CWE-521 | CWE-521 CWE-521 | CWE-521 CWE-521 Weak Password Requirements

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Horner Automation	Cscape	affected 10.0	Not specified
CNA	Horner Automation	XL7 PLC	affected 15.60	Not specified

CNA	Horner Automation	XL4 PLC	affected 16.32.0	Not specified

References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-10...	ics-cert@hq.dhs.gov	github.com	
www.cisa.gov/news-events/ics-advisories/icsa-26-106-02	ics-cert@hq.dhs.gov	www.cisa.gov	
hornerautomation.com/cscape-software-free/cscape-software	ics-cert@hq.dhs.gov	hornerautomation.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: An anonymous researcher reported this vulnerability to CISA (en)

Additional Advisory Data

Solutions

CNA: Horner Automation recommends users update to Cscape v10.2 SP2 or later. Horner Automation has also released the latest firmware for both XL4 and XL7 PLCs. Horner recommends users update to the latest version of the firmware. https://hornerautomation.com/cscape-software-free/cscape-software/

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