Hirschmann HiOS HiSecOS Authentication Bypass via HTTP Management

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-25236
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 23:17:00 UTC
Updated	2026-04-03 23:17:00 UTC
Description	Hirschmann HiOS and HiSecOS products RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED, EAGLE contain a

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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

Problem Types: CWE-287 | CWE-287 Improper Authentication (CWE-287)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
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:H/SC:N/SI:N/S
3.1	disclosure@vulncheck.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

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:H/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

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Belden	Hirschmann HiOS	affected 05.07 custom	Not specified
CNA	Belden	Hirschmann HiOS	affected 06.1.04 custom	Not specified
CNA	Belden	Hirschmann HiOS	affected 06.2.00 custom	Not specified
CNA	Belden	Hirschmann HiOS	unaffected 06.1.05 custom	Not specified

CNA	Belden	Hirschmann HiOS	unaffected 07.0.00 semver	Not specified
CNA	Belden	Hirschmann HiOS	unaffected 03.1.00 semver	Not specified
CNA	Belden	Hirschmann HiSecOS EAGLE	affected 03.00.02 semver	Not specified
CNA	Belden	Hirschmann HiSecOS EAGLE	unaffected 03.0.03 semver	Not specified

References

Reference	Source	Link
assets.belden.com/m/52ecadbb5f1b0e04/original/Security-Bulletin-Web-Server-Auth...	disclosure@vulncheck.com	assets.belden.com
www.vulncheck.com/advisories/hirschmann-hios-hisecos-authentication-bypass-via-...	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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