



CVE-2020-6994

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6994
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-03 19:15:00 UTC
Updated	2021-06-17 17:22:00 UTC
Description	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Belden	Hirschmann Eagle20	-	All	All	All
Hardware	Belden	Hirschmann Eagle30	-	All	All	All
Hardware	Belden	Hirschmann Embedded Ethernet Switch	-	All	All	All
Hardware	Belden	Hirschmann Embedded Ethernet Switch Extended	-	All	All	All
Hardware	Belden	Hirschmann Greyhound Swtich	-	All	All	All
Operating System	Belden	Hirschmann Hios	All	All	All	All
Operating System	Belden	Hirschmann Hisecos	All	All	All	All
Hardware	Belden	Hirschmann Mice Switch Power	-	All	All	All
Hardware	Belden	Hirschmann Octopus	-	All	All	All
Hardware	Belden	Hirschmann Prp Redbox	-	All	All	All
Hardware	Belden	Hirschmann Rail Switch Power	-	All	All	All
Hardware	Belden	Hirschmann Rail Switch Power Enhanced	-	All	All	All
Hardware	Belden	Hirschmann Rail Switch Power Lite	-	All	All	All
Hardware	Belden	Hirschmann Rail Switch Power Smart	-	All	All	All
Hardware	Hirschmann	Eagle20	-	All	All	All
Hardware	Hirschmann	Eagle20	-	All	All	All
Hardware	Hirschmann	Eagle30	-	All	All	All

Hardware	Hirschmann	Eagle30	-	All	All	All
Hardware	Hirschmann	Embedded Ethernet Switch	-	All	All	All
Hardware	Hirschmann	Embedded Ethernet Switch	-	All	All	All
Hardware	Hirschmann	Embedded Ethernet Switch Extended	-	All	All	All
Hardware	Hirschmann	Embedded Ethernet Switch Extended	-	All	All	All
Hardware	Hirschmann	Greyhound Swtich	-	All	All	All
Hardware	Hirschmann	Greyhound Swtich	-	All	All	All
Operating System	Hirschmann	Hios	All	All	All	All
Operating System	Hirschmann	Hisecos	All	All	All	All
Hardware	Hirschmann	Mice Switch Power	-	All	All	All
Hardware	Hirschmann	Mice Switch Power	-	All	All	All
Hardware	Hirschmann	Octopus	-	All	All	All
Hardware	Hirschmann	Octopus	-	All	All	All
Hardware	Hirschmann	Prp Redbox	-	All	All	All
Hardware	Hirschmann	Prp Redbox	-	All	All	All
Hardware	Hirschmann	Rail Switch Power	-	All	All	All
Hardware	Hirschmann	Rail Switch Power	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Enhanced	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Enhanced	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Lite	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Lite	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Smart	-	All	All	All
Hardware	Hirschmann	Rail Switch Power Smart	-	All	All	All

References

Reference	Source	Link	Tags
Hirschmann Automation and Control HiOS and HiSecOS Products CISA	MISC	www.us-cert.gov	Mitigation, Third Party Advisory, I
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591151](#) Hitachi Energy AFS660/AFS665 Vulnerability (ICSA-22-270-01,8DBD000122)

[591366](#) Hitachi Energy AFF660/665 Series Stack-based Buffer Overflow Vulnerability (ICSA-22-263-02, 8DBD000122)

© [CVE.report](#) 2026 |

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](#)