



Remote Code Execution Vulnerability in Hitachi Storage Navigator and the maintenance console

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

Summary

CVE	CVE-2025-1978
State	PUBLISHED
Assigner	Hitachi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 09:16:26 UTC
Updated	2026-05-07 09:16:26 UTC
Description	Remote Code Execution Vulnerability in Hitachi Storage Navigator and the maintenance console in Hitachi Virtual Storage I

Risk And Classification

Primary CVSS: v3.1 8.3 HIGH from hirt@hitachi.co.jp

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

Problem Types: CWE-94 | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	hirt@hitachi.co.jp	Secondary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Hitachi	Hitachi Virtual Storage Platform G130 G150 G350 G370 G700 G900 F350 F370 F700 F900	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform G130 G150 G350 G370 G700 G900 F350 F370 F700 F900	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform G130 G150 G350 G370 G700 G900 F350 F370 F700 F900	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform G130 G150 G350 G370 G700 G900 F350 F370 F700 F900	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform G130 G150 G350 G370 G700 G900 F350 F370 F700 F900	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform E390 E590 E790 E990 E1090 E390H E590H E790H E1090H	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform E390 E590 E790 E990 E1090 E390H E590H E790H E1090H	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform E390 E590 E790 E990 E1090 E390H E590H E790H E1090H	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform E390 E590 E790 E990 E1090 E390H E590H E790H E1090H	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform E390 E590 E790 E990 E1090 E390H E590H E790H E1090H	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform One Block 23 One Block 24 One Block 26 One Block 28	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform One Block 23 One Block 24 One Block 26 One Block 28	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform One Block 23 One Block 24 One Block 26 One Block 28	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform One Block 23 One Block 24 One Block 26 One Block 28	affected DKCMAIN Ver.
CNA	Hitachi	Hitachi Virtual Storage Platform One Block 23 One Block 24 One Block 26 One Block 28	affected DKCMAIN Ver.

References

Reference	Source	Link	Tags
www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_307.html	hirt@hitachi.co.jp	www.hitachi.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Thomas Josef Riedmaier, Siemens Energy. (en)

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)