



Buffer Overflow Vulnerability in JP1/IT Desktop Management 2 and JP1/NETM/DM

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

Summary

CVE	CVE-2025-65116
State	PUBLISHED
Assigner	Hitachi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 06:16:41 UTC
Updated	2026-04-07 13:20:11 UTC
Description	Buffer Overflow Vulnerability in JP1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management 2 - O

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from hirt@hitachi.co.jp

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

EPSS: 0.000130000 probability, percentile 0.020950000 (date 2026-04-07)

Problem Types: CWE-763 | CWE-763 CWE-763 Release of invalid pointer or reference

Version	Source	Type	Score	Severity	Vector
3.1	hirt@hitachi.co.jp	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 13-50 13-50-02 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 13-11 13-11-04 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 13-10 13-10-07 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 13-01 13-01-07 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 13-00 13-00-05 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 12-60 12-60-12 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Manager	affected 10-50 12-50-11 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 13-50 13-50-02 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 13-11 13-11-04 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 13-10 13-10-07 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 13-01 13-01-07 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 13-00 13-00-05 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 12-60 12-60-12 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management 2 - Operations Director	affected 10-50 12-50-11 custom	Windows
CNA	Hitachi	Job Management Partner 1/IT Desktop Management 2 - Manager	affected 10-50 10-50-11 custom	Windows
CNA	Hitachi	JP1/IT Desktop Management - Manager	affected 09-50 10-10-16 custom	Windows
CNA	Hitachi	Job Management Partner 1/IT Desktop Management - Manager	affected 09-50 10-10-16 custom	Windows
CNA	Hitachi	JP1/NETM/DM Manager	affected 09-00 10-20-02 custom	Windows
CNA	Hitachi	JP1/NETM/DM Client	affected 09-00 10-20-02 custom	Windows
CNA	Hitachi	Job Management Partner 1/Software Distribution Manager	affected 09-00 09-51-13 custom	Windows
CNA	Hitachi	Job Management Partner 1/Software Distribution Client	affected 09-00 09-51-13 custom	Windows

References

Reference	Source	Link	Tags
www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-118/...	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: Ruslan Sayfiev (en)

CNA: Denis Faiustov (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](#)