



# CVE-2026-33566

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

## Summary

<b>CVE</b>	CVE-2026-33566
<b>State</b>	PUBLISHED
<b>Assigner</b>	jpcert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 00:16:20 UTC
<b>Updated</b>	2026-04-27 00:16:20 UTC
<b>Description</b>	There is a cypher injection issue in LogonTracer prior to v2.0.0. If specially crafted Windows event log data is loaded, the c

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from vultures@jpcert.or.jp

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-943 | CWE-943 Improper Neutralization of Special Elements in Data Query Logic

Version	Source	Type	Score	Severity	Vector
4.0	vultures@jpcert.or.jp	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
3.0	vultures@jpcert.or.jp	Secondary	4.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.0	CNA	CVSS	4.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Japan Computer Emergency Response Team Coordination Center JPCERTCC	LogonTracer	affected prior to v2.0.0	Not spec

### References

Reference	Source	Link	Tags
...	...	...	...

<a href="https://jvn.jp/en/jp/JVN57877356">jvn.jp/en/jp/JVN57877356</a>	<a href="mailto:vultures@jpcert.or.jp">vultures@jpcert.or.jp</a>	<a href="https://jvn.jp">jvn.jp</a>	
<a href="https://www.jpcert.or.jp/press/2026/PR20260423.html">www.jpcert.or.jp/press/2026/PR20260423.html</a>	<a href="mailto:vultures@jpcert.or.jp">vultures@jpcert.or.jp</a>	<a href="https://www.jpcert.or.jp">www.jpcert.or.jp</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)