CVE-2026-33566

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33566
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 00:16:20 UTC
Updated	2026-04-27 00:16:20 UTC
Description	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/MSC:X/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/MSC:X/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

jvn.jp/en/jp/JVN57877356	vultures@jpcert.or.jp	jvn.jp	
www.jpcert.or.jp/press/2026/PR20260423.html	vultures@jpcert.or.jp	www.jpcert.or.jp	
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.

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