CVE-2025-1790

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

Summary

CVE	CVE-2025-1790
State	PUBLISHED
Assigner	Genetec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-13 17:16:10 UTC
Updated	2026-04-26 18:49:06 UTC
Description	Local privilege escalation in Genetec Sipelia Plugin. An authenticated low-privileged Windows user could exploit this vulner

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from security@genetec.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:U/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:P/AU:N/R:X/V:C/RE:X/U:X

EPSS: 0.000210000 probability, percentile 0.058850000 (date 2026-04-26)

Problem Types: CWE-250 | CWE-250 Execution with Unnecessary Privileges

Version	Source	Type	Score	Severity	Vector
4.0	security@genetec.com	Secondary	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:
4.0	CNA	CVSS	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

ntegrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:U/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:P/AU:N/R:X/V:C/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Genetec Inc.	Genetec Sipelia	affected <2.14.271 semver	Windows
CNA	Genetec Inc.	Genetec Sipelia	unaffected >=2.14.271 semver	Windows

References

Reference	Source	Link	Tags
techdocs.genetec.com/r/en-US/Security-Updates-for-SipeliaTM-2.14	security@genetec.com	techdocs.genetec.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: Rutger Flohil (en)

Additional Advisory Data

Solutions

CNA: Hotfix 2.14.271 must be installed on client and server machines to resolve this issue. This issue will also be fixed in all later versions.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report