CVE-2025-1789

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

Summary

CVE	CVE-2025-1789
State	PUBLISHED
Assigner	Genetec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-24 20:27:42 UTC
Updated	2026-04-26 18:49:06 UTC
Description	Local privilege escalation in Genetec Update Service. An authenticated, low-privileged, Windows user could exploit this vul

Risk And Classification

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

CVSS:4.0/AV:L/AC:H/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: 0.000140000 probability, percentile 0.027610000 (date 2026-04-26)

Problem Types: CWE-276 | CWE-276 Incorrect Default Permissions

Version	Source	Type	Score	Severity	Vector
4.0	security@genetec.com	Secondary	5.8	MEDIUM	CVSS:4.0/AV:L/AC:H/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:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:H/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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Genetec	Genetec Update Service	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Genetec Inc.	Genetec Update Service	affected <2.10.600 semver	Windows
CNA	Genetec Inc.	Genetec Update Service	unaffected >= 2.10.600 semver	Windows

CNA	Genetec Inc.	Genetec Update Service	unaffected >=2.10.600 semver	Windows

References

Reference	Source	Link
techdocs.genetec.com/r/en-US/Security-Updates-for-GenetecTM-Update-Service-2.10/Re...	security@genetec.com	techdocs.genetec.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Rutger Flohil (en)

Additional Advisory Data

Solutions

CNA: This issue is fixed in Genetec Update Service 2.10.600 and all later versions. Internet connected Genetec Update Service will automatically update themselves.

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