



# CVE-2025-1787

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

## Summary

<b>CVE</b>	CVE-2025-1787
<b>State</b>	PUBLISHED
<b>Assigner</b>	Genetec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-24 20:27:42 UTC
<b>Updated</b>	2026-04-26 18:49:05 UTC
<b>Description</b>	Local admin could to leak information from the Genetec Update Service configuration web page. An authenticated, admin p

## 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/MSX/MSI:X/MSA:X/S:P/AU:N/R:X/V:C/RE:X/U:X

**EPSS:** 0.000090000 probability, percentile 0.009750000 (date 2026-04-26)

**Problem Types:** CWE-346 | CWE-346 CWE-346: Origin Validation Error

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

## 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/MSG: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

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

### 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

## References

Reference	Source	Link
<a href="https://techdocs.genetec.com/r/en-US/Security-Updates-for-GenetecTM-Update-Service-2.10/Re...">techdocs.genetec.com/r/en-US/Security-Updates-for-GenetecTM-Update-Service-2.10/Re...</a>	<a href="mailto:security@genetec.com">security@genetec.com</a>	<a href="https://techdocs.genetec.com">techdocs.genetec.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

## 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.

© [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](https://cve.report/api)

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