Windows Hello Security Feature Bypass Vulnerability

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

Summary

CVE	CVE-2026-27928
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 18:17:04 UTC
Updated	2026-04-22 17:36:40 UTC
Description	Improper input validation in Windows Hello allows an unauthorized attacker to bypass a security feature over a network.

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from secure@microsoft.com

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

EPSS: 0.000780000 probability, percentile 0.233030000 (date 2026-04-22)

Problem Types: CWE-20 | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	8.7	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2019	All	All	All	All
Operating System	Microsoft	Windows Server 2022	All	All	All	All
Operating System	Microsoft	Windows Server 2022 23h2	All	All	All	All
Operating System	Microsoft	Windows Server 2025	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfc
CNA	Microsoft	Windows Server 2016	affected 10.0.14393.0 10.0.14393.9060 custom	x64-b
CNA	Microsoft	Windows Server 2016 Server Core Installation	affected 10.0.14393.0 10.0.14393.9060 custom	x64-b
CNA	Microsoft	Windows Server 2019	affected 10.0.17763.0 10.0.17763.8644 custom	x64-b
CNA	Microsoft	Windows Server 2019 Server Core Installation	affected 10.0.17763.0 10.0.17763.8644 custom	x64-b
CNA	Microsoft	Windows Server 2022	affected 10.0.20348.0 10.0.20348.5020 custom	x64-b
CNA	Microsoft	Windows Server 2022 23H2 Edition Server Core Installation	affected 10.0.25398.0 10.0.25398.2274 custom	x64-b
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32690 custom	x64-b

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-27928	secure@microsoft.com	msrc.microsoft.com	Vendor Advisory
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.

Free CVE JSON API cve.report/api

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