CVE-2026-8142

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

Summary

CVE	CVE-2026-8142
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 20:16:45 UTC
Updated	2026-05-08 14:16:48 UTC
Description	VINCE versions 3.0.38 and earlier do not properly verify the From address authenticity due to encoding confusion and use t

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.000140000 probability, percentile 0.026180000 (date 2026-05-09)

Problem Types: CWE-345: Insufficient Verification of Data Authenticity

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CERTCC	VINCE	affected 3.0.38 semver	Not specified

References

Reference	Source	Link	Tags
github.com/CERTCC/VINCE	cret@cert.org	github.com	
kb.cert.org/vince	cret@cert.org	kb.cert.org	
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: Thanks to Guillem Lefait guillem@datamq.com for reporting the issue (en)

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