CVE-2006-0536

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

Summary

CVE	CVE-2006-0536
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-04 00:06:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cross-site scripting (XSS) vulnerability in neomail.pl in NeoMail 1.27 allows remote attackers to inject arbitrary web script or

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS: 0.006130000 probability, percentile 0.698890000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Neomail	Neomail	1.27	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
www.osvdb.org/22978	af854a3a-2127-422b
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b
SecurityFocus	af854a3a-2127-422b
IBM X-Force Exchange	af854a3a-2127-422b
SecurityTracker.com Archives - NeoMail Input Validation Flaw in 'date' Parameter Permits Cross-Site Scripting Attacks	af854a3a-2127-422b
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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