CVE-2008-1532

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

Summary

CVE	CVE-2008-1532
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-28 00:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Perlbal before 1.70, when buffered upload is enabled, allows remote attackers to cause a denial of service (crash) via a zer

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Perlbal	Perlbal	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Bug 439054 – CVE-2008-1532 Perlbal crashes upon empty buffered upload attempts
[SECURITY] Fedora 7 Update: Perlbal-1.70-1.fc7
IBM X-Force Exchange
Gentoo Bug 214784 - dev-perl/Perlbal <1.70 crash on zero byte chunked upload when buffered uploads are enabled (CVE-2008-{1532,1652})
Perlbal Buffered Upload Remote Denial Of Service Vulnerability
Perlbal Chunked Uploads Denial of Service and Directory Traversal - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
search.cpan.org/src/BRADFITZ/Perlbal-1.70/CHANGES
[SECURITY] Fedora 8 Update: Perlbal-1.70-1.fc8
Fedora update for Perlbal - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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