CVE-2006-2093

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

Summary

CVE	CVE-2006-2093
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-29 10:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Nessus before 2.2.8, and 3.x before 3.0.3, allows user-assisted attackers to cause a denial of service (memory consumptio

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

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

EPSS: 0.010850000 probability, percentile 0.779260000 (date 2026-04-17)

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Nessus	Nessus	2.2.0	All	All	All
Application	Nessus	Nessus	2.2.0_rc1	All	All	All
Application	Nessus	Nessus	2.2.1	All	All	All
Application	Nessus	Nessus	2.2.2	All	All	All
Application	Nessus	Nessus	2.2.3	All	All	All
Application	Nessus	Nessus	2.2.5	All	All	All
Application	Nessus	Nessus	2.2.6	All	All	All
Application	Nessus	Nessus	All	All	All	All
Application	Nessus	Nessus	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
SecurityFocus	af854a3a-2127-422b-91ae-364da
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da
SecurityFocus	af854a3a-2127-422b-91ae-364da
USN-279-1: libnasl/nessus vulnerability | Ubuntu security notices	af854a3a-2127-422b-91ae-364da
SecurityFocus	af854a3a-2127-422b-91ae-364da
www.osvdb.org/25084	af854a3a-2127-422b-91ae-364da
Nessus libnasl split() Function Buffer Overflow May Let Authorized Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da
SecurityReason - NASL 'Split' function Buffer overflow	af854a3a-2127-422b-91ae-364da
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da
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.

Free CVE JSON API cve.report/api

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