CVE-2007-0166

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

Summary

CVE	CVE-2007-0166
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-11 20:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The jail rc.d script in FreeBSD 5.3 up to 6.2 does not verify pathnames when writing to /var/log/console.log during a jail star

Risk And Classification

Primary CVSS: v2.0 6.6 from nvd@nist.gov

AV:L/AC:M/Au:S/C:C/I:C/A:C

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	5.3	All	All	All

Operating System	Freebsd	Freebsd	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
security.freebsd.org/advisories/FreeBSD-SA-07:01.jail.asc	af854a3a-2127-422
FreeBSD Jail RC.D Multiple Local Symbolic Link Vulnerabilities	af854a3a-2127-422
FreeBSD jail rc.d Security Bypass Vulnerability - Advisories - Secunia	af854a3a-2127-422
osvdb.org/32726	af854a3a-2127-422
SecurityTracker.com Archives - FreeBSD Kernel jail(2) Call Lets Local Users Gain Elevated Privileges in Certain Cases	af854a3a-2127-422
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.