CVE-2011-4062

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

Summary

CVE	CVE-2011-4062
State	PUBLIC
Assigner	secteam@freebsd.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-10-18 01:55:00 UTC
Updated	2011-12-13 04:09:00 UTC
Description	Buffer overflow in the kernel in FreeBSD 7.3 through 9.0-RC1 allows local users to cause a denial of service (panic) or poss

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	7.3	All	All	All
Operating System	Freebsd	Freebsd	7.4	All	All	All
Operating System	Freebsd	Freebsd	8.1	All	All	All
Operating System	Freebsd	Freebsd	8.2	All	All	All
Operating System	Freebsd	Freebsd	9.0	beta1	All	All
Operating System	Freebsd	Freebsd	9.0	beta2	All	All
Operating System	Freebsd	Freebsd	9.0	beta3	All	All
Operating System	Freebsd	Freebsd	7.3	All	All	All
Operating System	Freebsd	Freebsd	7.4	All	All	All
Operating System	Freebsd	Freebsd	8.1	All	All	All
Operating System	Freebsd	Freebsd	8.2	All	All	All
Operating System	Freebsd	Freebsd	9.0	beta1	All	All
Operating System	Freebsd	Freebsd	9.0	beta2	All	All
Operating System	Freebsd	Freebsd	9.0	beta3	All	All

References

Reference	Source	Link

FreeBSD UNIX-Domain Socket Buffer Overflow Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.securitytr
FreeBSD UIPC socket heap overflow proof-of-concept	EXPLOIT-DB	www.exploit-db
FreeBSD-SA-11:05	FREEBSD	security.freebs
Security Advisory SA46564 - Debian update for kfreebsd-8 - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-2325-1 kfreebsd-8	DEBIAN	www.debian.or
FreeBSD UNIX Domain Socket Handling Privilege Escalation Vulnerability - Secunia.com	SECUNIA	secunia.com
security.freebsd.org/patches/SA-11:05/unix2.patch	MISC	security.freebs
FreeBSD UNIX Domain Socket Local Privilege Escalation Vulnerabiity	BID	www.securityfo
75788	OSVDB	www.osvdb.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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