CVE-2000-0916

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

Summary

CVE	CVE-2000-0916
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-12-19 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	FreeBSD 4.1.1 and earlier, and possibly other BSD-based OSes, uses an insufficient random number generator to generate

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	2.0	All	All	All

Operating System	Freebsd	Freebsd	3.0	All	All	All
Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	4.1	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
BSD Weak initial Sequence Number Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfoc
ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-00:52.tcp-iss.asc	af854a3a-2127-422b-91ae-364da2661108	ftp.freebsd.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.