



CVE-2000-0535

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

Summary

CVE	CVE-2000-0535
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-06-12 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	OpenSSL 0.9.4 and OpenSSH for FreeBSD do not properly check for the existence of the /dev/random or /dev/urandom de

Risk And Classification

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

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	4.0	alpha	All	All

Operating System	Freebsd	Freebsd	5.0	alpha	All	All
Application	Openssl	Openssl	0.9.4	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		
archives.neohapsis.com/archives/freebsd/2000-06/0083.html			af854a3a-2127-422b-91ae-364da2661108	archives.neohapsis		
FreeBSD Alpha Port Lack Of /dev/random and /dev/urandom Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.		
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.						