CVE-2001-1141

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2001-1141
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-10 04:00:00 UTC
Updated	2017-10-10 01:30:00 UTC
Description	The Pseudo-Random Number Generator (PRNG) in SSLeay and OpenSSL before 0.9.6b allows attackers to use the outpu

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Ssleay	Ssleay	0.8.1	All	All	All
Application	Ssleay	Ssleay	0.9	All	All	All
Application	Ssleay	Ssleay	0.9.1	All	All	All

Application	Ssleay	Ssleay	0.8.1	All	All	All
Application	Ssleay	Ssleay	0.9	All	All	All
Application	Ssleay	Ssleay	0.9.1	All	All	All

References

Reference	Source	Link	Tags
SecurityFocus	BUGTRAQ	www.securityfocus.com	Patch, Vendor Advisory
404 Not Found	OSVDB	www.osvdb.org	
OpenSSL PRNG Internal State Disclosure Vulnerability	BID	www.securityfocus.com	Patch, Vendor Advisory
redhat.com | Red Hat Support	REDHAT	www.redhat.com	Patch, Vendor Advisory
NetBSD-SA2001-013	NETBSD	ftp.netbsd.org	
FreeBSD-SA-01:51	FREEBSD	www.securityfocus.com	
Home - Conectiva	CONECTIVA	distro.conectiva.com.br	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
LinuxSecurity.com: EnGarde: 'openssl' PRNG weakness	ENGARDE	www.linuxsecurity.com	
MandrakeSoft Update Advisory MDKSA-2001:065 : openssl	MANDRAKE	www.linux-mandrake.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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