CVE-2020-1968

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1968
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 14:15:00 UTC
Updated	2022-11-21 19:48:00 UTC
Description	The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-ma

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Hardware	Fujitsu	M10-1	-	All	All	All
Operating System	Fujitsu	M10-1 Firmware	All	All	All	All
Hardware	Fujitsu	M10-4	-	All	All	All
Hardware	Fujitsu	M10-4s	-	All	All	All
Operating System	Fujitsu	M10-4s Firmware	All	All	All	All
Operating System	Fujitsu	M10-4 Firmware	All	All	All	All
Hardware	Fujitsu	M12-1	-	All	All	All
Operating System	Fujitsu	M12-1 Firmware	All	All	All	All
Hardware	Fujitsu	M12-2	-	All	All	All
Hardware	Fujitsu	M12-2s	-	All	All	All
Operating System	Fujitsu	M12-2s Firmware	All	All	All	All

Operating System	Fujitsu	M12-2 Firmware	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Hardware	Oracle	Ethernet Switch Es1-24	-	All	All	All
Operating System	Oracle	Ethernet Switch Es1-24 Firmware	1.3.1	All	All	All
Hardware	Oracle	Ethernet Switch Es2-64	-	All	All	All
Operating System	Oracle	Ethernet Switch Es2-64 Firmware	2.0.0.14	All	All	All
Hardware	Oracle	Ethernet Switch Es2-72	-	All	All	All
Operating System	Oracle	Ethernet Switch Es2-72 Firmware	2.0.0.14	All	All	All
Hardware	Oracle	Ethernet Switch Tor-72	-	All	All	All
Operating System	Oracle	Ethernet Switch Tor-72 Firmware	1.2.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
OpenSSL: Multiple Vulnerabilities (GLSA 202210-02) — Gentoo security	GENTOO	security.gentoo.org	
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle.com	
www.openssl.org/news/secadv/20200909.txt	CONFIRM	www.openssl.org	Vendor Advisory
CVE-2020-1968 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party Advis
USN-4504-1: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advis
[SECURITY] [DLA 2378-1] openssl1.0 security update	MLIST	lists.debian.org	Mailing List, Thir
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

Vendor Comments And Credit

Discovery Credit

LEGACY: Robert Merget, Marcus Brinkmann, Nimrod Aviram, and Juraj Somorovsky

Legacy QID Mappings

330079 IBM AIX Multiple Vulnerabilities in Openssl (openssl_advisory32)

374875 Oracle PeopleSoft Enterprise PeopleTools Multiple vulnerabilitites (CPUJAN2021)

591018 Hitachi Energy RTU500 series Multiple Vulnerabilities (ICSA-21-336-08)

710638 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202210-02)

730319 Palo Alto Networks (PAN-OS) Impact of the Raccoon Attack Vulnerability (PAN-154936)

91781 IBM Integration Bus and IBM App Connect Enterprise Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (6444817,6444819)