CVE-2015-5738

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-5738
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-26 17:59:00 UTC
Updated	2023-08-16 14:17:00 UTC
Description	The RSA-CRT implementation in the Cavium Software Development Kit (SDK) 2.x, when used on OCTEON II CN6xxx Hard

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Traffix Sdc	All	All	All	All
Application	F5	Traffix Sdc	All	All	All	All
Application	F5	Traffix Signaling Delivery Controller	All	All	All	All
Application	F5	Traffix Signaling Delivery Controller	All	All	All	All
Hardware	Marvell	Octeon Ii Cn6000	-	All	All	All
Hardware	Marvell	Octeon Ii Cn6000	-	All	All	All
Hardware	Marvell	Octeon Ii Cn6010	-	All	All	All
Hardware	Marvell	Octeon Ii Cn6010	-	All	All	All
Hardware	Marvell	Octeon Ii Cn6020	-	All	All	All
Hardware	Marvell	Octeon Ii Cn6020	-	All	All	All
Application	Marvell	Software Development Kit	2.0	All	All	All
Application	Marvell	Software Development Kit	2.0	All	All	All

References

Reference	Source	Link	Tags
people.redhat.com/~fweimer/rsa-crt-leaks.pdf	MISC	people.redhat.com	Technical Description, Third Party Advis
RSA-CRT key leak under certain conditions | FortiGuard.com	CONFIRM	fortiguard.com	Broken Link

SOL91245485 - RSA-CRT key leak vulnerability CVE-2015-5738	CONFIRM	support.f5.com	Third Party Advisory
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.

Legacy QID Mappings

900089 CBL-Mariner Linux Security Update for kernel 5.4.51

903041 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3480)

906203 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3480-1)