



# CVE-2015-5738

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

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

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Traffic Sdc	All	All	All	All
Application	F5	Traffic Sdc	All	All	All	All
Application	F5	Traffic Signaling Delivery Controller	All	All	All	All
Application	F5	Traffic Signaling Delivery Controller	All	All	All	All
Hardware	Marvell	Octeon li Cn6000	-	All	All	All
Hardware	Marvell	Octeon li Cn6000	-	All	All	All
Hardware	Marvell	Octeon li Cn6010	-	All	All	All
Hardware	Marvell	Octeon li Cn6010	-	All	All	All
Hardware	Marvell	Octeon li Cn6020	-	All	All	All
Hardware	Marvell	Octeon li 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	<a href="https://people.redhat.com/~fweimer/rsa-crt-leaks.pdf">people.redhat.com</a>	Technical Description, Third Party Advis
RSA-CRT key leak under certain conditions   FortiGuard.com	CONFIRM	<a href="https://fortiguard.com">fortiguard.com</a>	Broken Link

SOL91245485 - RSA-CRT key leak vulnerability CVE-2015-5738	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)