ID 20180601 FAQ

Vulnerabilities in Openssl – CVE-2017-3738 CVE-2018-0733 & CVE-2018-0739

Initial Internal Release Date: **06/01/2018**
Initial Release to the public**: 06/01/2018**
Update Release Date: **06/01/2018**

This "Ruckus Networks Security Advisory" constitutes Ruckus Networks (an ARRIS company) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Networks (an ARRIS company).

What are the issues?

The following security advisory was published by OpenSSL on 23rd Mar 2018 https://www.openssl.org/news/secadv/20180327.txt While the advisory refers to more vulnerabilities, Ruckus addresses only High and Moderate vulnerabilities.

These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

SNo.	CVE-ID	CVE Description
1	CVE-2017-3738	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected.
2	CVE-2018-0733	Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. The module can only be compiled by the HP-UX assembler, so that only HP-UX PA-RISC targets are affected.
3	CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack.

What is the impact of these on Ruckus products?

Various versions of OpenSSL are used in all Ruckus products, namely SmartZone(SZ/SCG) family of products, AP product line, Zone Director (ZD) product line, Flex Master, SCI, SPoT products. One or more versions of SW for these products are impacted by these vulnerabilities. However, the exploitability and actual impact on Ruckus products varies based on use cases. Details below describe each vulnerability.

CVE-2017-3738: Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. The resources needed to attack DH1024 is also very significant. Furthermore, this only affects processors that support the AVX2 but not ADX extensions like Intel Haswell(4th Gen) Hence the exploitability of this issue is very low.

© 2018 Ruckus Networks (an ARRIS company).

ID 20180601 FAQ

CVE-2018-0733: The module can only be compiled by the HP-UX assembler, so that only HP-UX PA-RISC targets are affected. Hence it is not applicable to Ruckus products.

CVE-2018-0739: There are no such recursive structures used within SSL/TLS that come from untrusted sources so this is considered safe. Hence exploitability is very low.

Overall, none of these vulnerabilities are easily exploitable on Ruckus solutions. Though this issue is not exploitable on Ruckus products, we will be rolling out the OpenSSL updates in SZ releases and ZD releases. All future releases will contain the newer version of OpenSSL.

Do I need to check if I am vulnerable?
There is no need to check for this as Ruckus confirms using versions of OpenSSL impacted in some products.

How does Ruckus qualify severity of security issues?
Ruckus Wireless typically utilizes the Common Vulnerability Scoring System (CVSS) v3. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. In cases where CVSS v3 scores are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2017-3738	5.9 (Medium)	(AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2018-0733	5.9 (Medium)	(AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)
CVE-2018-0739	6.5 (Medium)	(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

When will this Ruckus Security Advisory be publicly posted?
Ruckus Wireless released the initial security advisory to Ruckus field teams on: 06/01/2018
Ruckus Wireless released the initial security advisory to customers on: 06/01/2018
Public posting: 06/01/2018

Revision History

Version	ID	Change	Date
1.0	20180601	Initial Release	June 01, 2018

Ruckus Support can be contacted as follows:
The full contact list is at: https://support.ruckuswireless.com/contact-us

DISCLAIMER
THIS RUCKUS Networks SECURITY ADVISORY INCLUDING THE INFORMATION IT CONTAINS AND THE PROGRAMS MADE AVAILABLE THROUGH THE LINKS THAT IT INCLUDES, IS PROVIDED TO YOU ON AN "AS IS" BASIS. RUCKUS NETWORKS (AN ARRIS COMPANY) AND ITS SUPPLIERS DO NOT

© 2018 Ruckus Networks (an ARRIS company).

ID 20180601 FAQ

WARRANT THAT SUCH INFORMATION OR THE FUNCTIONS CONTAINED IN SUCH PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR-FREE. THE INFORMATION AND PROGRAMS ARE PROVIDED TO YOU WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT WILL RUCKUS NETWORKS (AN ARRIS COMPANY), ITS SUPPLIERS, OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE INFORMATION OR PROGRAMS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, THAT MAY ARISE OUT OF YOUR USE OF OR FAILURE TO USE THE INFORMATION OR PROGRAMS, EVEN IF RUCKUS NETWORKS (AN ARRIS COMPANY) OR SUCH OTHER ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL NOT BE DEEMED TO PRECLUDE ANY LIABILITY, WHICH UNDER APPLICABLE PRODUCTS LIABILITY LAW, CANNOT BE PRECLUDED BY CONTRACT.

This “Ruckus Networks Security Advisory” constitutes Ruckus Networks (an ARRIS company) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Networks (an ARRIS COMPANY).

© Copyright 2018 Ruckus Wireless (Part of Brocade Inc). All Rights Reserved