ID 20180226 FAQ

XSS vulnerability in Ruckus ICX FastIron – (CVE-2013-6786)

Initial Internal Release Date: **02/26/2018**
Initial Release to the public**: 02/26/2018**
Update Release Date: **02/26/2018**

Summary

Due to a Cross-site scripting (XSS) vulnerability, by requesting a nonexistent URI in a crafted HTTP Referrer header, arbitrary web scripts or HTML can be injected to the Ruckus FastIron device's web server.

What are the issues?

Due to XSS vulnerability in Allegro RomPage before 4.51, when the "forbidden author header" protection mechanism is bypassed, remote attackers may inject arbitrary web script or HTML by requesting a nonexistent URI in conjunction with a crafted HTTP Referrer header that is not properly handled in a 404 page.

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

SNo.	CVE-ID	CVE Description
1	CVE-2013-6786	Cross-site scripting (XSS) vulnerability in Allegro RomPager before 4.51, as used on the ZyXEL P660HW-D1, Huawei MT882, Sitecom WL-174, TP-LINK TD-8816, and D-Link DSL-2640R and DSL-2641R, when the "forbidden author header" protection mechanism is bypassed, allows remote attackers to inject arbitrary web script or HTML by requesting a nonexistent URI in conjunction with a crafted HTTP Referer header that is not properly handled in a 404 page

How do these vulnerabilities impact Ruckus products?

Ruckus ICX FastIron products running firmware 08.0.20a and above are impacted.

Below table provides the details of the area of impact of each CVE and affected Ruckus products:

Sno	CVE-ID	Impacted Area	Affected Ruckus Products	Comments
1	CVE-2013-6786	HTTP server	SX800, SX1600 (SXL) ICX – 6610, 6450, 6430, 7150, 7250, 7450, 7650, 7750	Affected Software versions: FI 08.0.20a and above

ID 20180226 FAQ

Are there any workarounds available?

No workarounds are available.

What release the fixes will be available?

Platform/Products	Release*	Target Release Date
ICX	FI 08.0.30r	03/30/2018
ICX	FI 08.0.61c	05/11/2018
ICX	FI 08.0.70b	03/19/2018

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-2013-6786	4.3 (Medium)	(AV:N/AC:M/Au:N/C:N/I:P/A:N) (legend)

When will this Ruckus Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: 02/26/2018
Ruckus Wireless released the initial security advisory to customers on: 02/26/2018
Public posting: 02/26/2016

Revision History

Version	ID	Change	Date
1.0	20180226	Initial Release	February 26, 2018

Ruckus Support can be contacted as follows:

The full contact list is at: https://support.ruckuswireless.com/contact-us

DISCLAIMER

ID 20180226 FAQ

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).