Security Advisory SWRX-2012-004

Juniper Mobility System Software (MSS™) web portal WebAAA cross-site scripting (XSS)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Juniper Mobility System Software (MSS™) web portal WebAAA cross-site scripting (XSS)
Advisory ID: SWRX-2012-004
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2012-004/
Date published: Thursday, June 14, 2012
CVE: CVE-2012-1038
CVSS v2 base score: 5.0
Date of last update: Thursday, August 22, 2013
Vendors contacted: Juniper Networks, Inc.
Release mode: Coordinated
Discovered by: Craig Lambert, Dell SecureWorks

Summary

The Juniper Networks Mobility System Software is part of Juniper's Wireless LAN Services (WLS) software product set and is the operating system component of the Mobility System[1]. According to the Mobility System Software configuration guide, the Mobility System Software runs all WLC switches and WLAs in a WLAN. This advisory focuses on the Juniper Mobility System Software web portal WebAAA, which "provides a simple and universal way to authenticate any user or device using a web browser. A common application of WebAAA is to control access for guests on your network."

A vulnerability exists in the WebAAA login function for versions prior to 7.6.3 and 7.7.1 due to insufficient input validation of arbitrary URL parameters. Successful exploitation may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

Affected products

This vulnerability affects supported versions of the Mobility System Software prior to 7.6.3 and 7.7.1. Unsupported versions prior to versions 7.5.3, 7.4 and 7.3 are also affected.

http://www.juniper.net/techpubs/en_US/release-independent/wireless/information-products/pathway-pages/wireless-lan/index.html

Vendor information, solutions and workarounds

The vendor has released an updated version to address this vulnerability. Users of the Mobility System Software should upgrade to versions 7.6.3 or 7.7.1.

---

[1] Juniper Networks documentation describes the Juniper Networks Mobility System as "an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The Juniper system provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices."

Juniper advisory: "2012-06 Security Bulletin: Mobility System Software (MSS): Parameter is not properly sanitized allowing XSS"

Details

A vulnerability exists in Mobility System Software versions prior to 7.6.3 and 7.7.1 due to insufficient input validation affecting the web portal WebAAA user login function. User-controllable input supplied to the wba_login.html page via an arbitrary parameter is not properly sanitized for illegal or malicious data prior to being returned to the user in dynamically generated web content. Remote attackers could leverage this issue to conduct reflected cross-site scripting (XSS) attacks via specially crafted requests. When loaded, arbitrary script or HTML code injected into the affected parameter will be executed in a target user's browser session in the security context of a vulnerable website. Successful exploitation may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

CVSS severity (version 2.0)

Access Vector: Network
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized modification
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
Impact Subscore: 2.9
Exploitability Subscore: 8.6
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Proof of concept

Request URL:

```
hxxps://webaaa.target/aaa/wba_login.html?wbaredirect=wba-dns-
error&9f45d”><script>alert(1)</script>22whatever=1
```

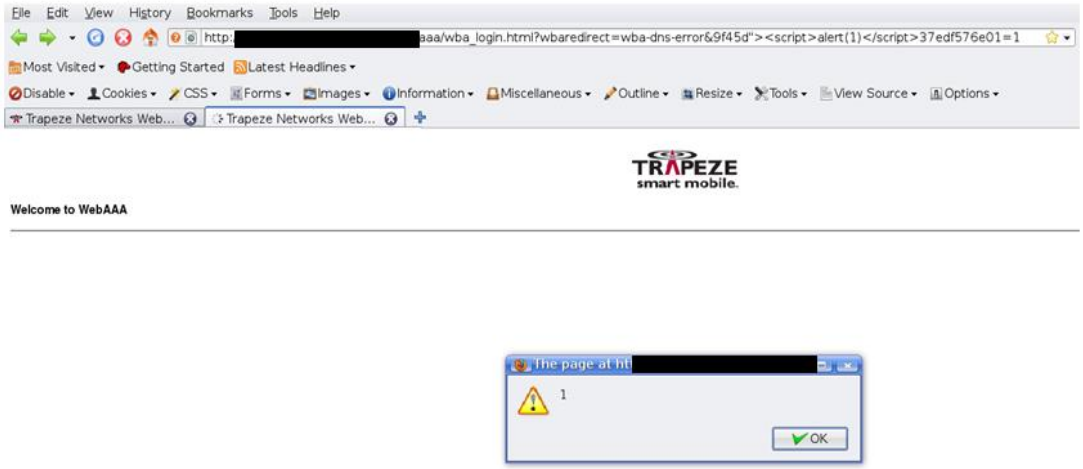

Figure 1. Screenshot of proof of concept.

Revision history

1.0 2012-06-14: Initial advisory release

1.1 2013-08-22: Update following Juniper's public advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer