	Authorisation. Jason Edelstein
	Release date. 10 September 2013.

Sense of Security – Security Advisory – SOS-13-003.

Juniper Junos J-Web Privilege Escalation Vulnerability.

10 September 2013.

Juniper Junos J-Web Privilege Escalation Vulnerability - Security Advisory - SOS-13-003

Release Date.	10-Sep-2013
Last Update.	-
Vendor Notification Date.	27-Sep-2012
Product.	Juniper Junos J-Web
Platform.	Junos
Affected versions.	All builds prior to 2013-02-28 are affected
Severity Rating.	Medium
Impact.	Privilege escalation
Attack Vector.	From remote with read-only authentication
Solution Status.	Vendor patch (not verified by SOS) Disable J-Web or limit access
CVE reference.	CVE- Not yet assigned

Details.

The J-Web is a GUI based network management application used on Junos devices.

The web application is vulnerable to a remote code execution vulnerability which permits privilege escalation. The file /jsdm/ajax/port.php allows execution of arbitrary user supplied PHP code via the rs POST parameter. Code executes with UID=0 (root) privileges, however you are confined to a chroot. Privilege escalation can be achieved by waiting for an administrator to log in and reading the contents of /tmp to hijack their session.

Proof of Concept.

Code execution: Execute a command inside the Chroot:

```
POST /jsdm/ajax/port.php
rs=exec&rsargs[]=echo “hello”
```

Privilege escalation: Read /tmp and hijack a session

```
POST /jsdm/ajax/port.php
rs=file_get_contents&rsargs[]=/tmp
```

Solution.

All Junos OS software releases built on or after 2013-02-28 have fixed this specific issue. This fix has not been validated by SOS.

As a workaround disable J-Web, or limit access to only trusted hosts.

This issue is being tracked as PR 826518 and is visible on the Juniper Customer Support website.

Discovered by.

Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-13-003.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php