



x

[Back to Article Page](#)

2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

[\[JSA10713\] Show KB Properties](#)

PRODUCT AFFECTED:

Please see below for details.

PROBLEM:

During an internal code review, two security issues were identified.

Administrative Access (CVE-2015-7755) allows unauthorized remote administrative access to the device. Exploitation of this vulnerability can lead to complete compromise of the affected device.

This issue only affects ScreenOS 6.3.0r17 through 6.3.0r20. No other Juniper products or versions of ScreenOS are affected by this issue.

Upon exploitation of this vulnerability, the log file would contain an entry that 'system' had logged on followed by password authentication for a username.

Example:

Normal login by user **username1**:

```
2015-12-17 09:00:00 system warn 00515 Admin user username1 has logged on via SSH from ....
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username1' at host ...
```

Compromised login by user **username2**:

```
2015-12-17 09:00:00 system warn 00515 Admin user system has logged on via SSH from ....
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username2' at host ...
```

Note that a skilled attacker would likely remove these entries from the local log file, thus effectively eliminating any reliable signature that the device had been compromised.

This issue has been assigned [CVE-2015-7755](#).

VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic. It is independent of the first issue.

This issue affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20. No other Juniper products or versions of ScreenOS are affected by this issue.

There is no way to detect that this vulnerability was exploited.

This issue has been assigned [CVE-2015-7756](#).

Juniper SIRT is not aware of any malicious exploitation of these vulnerabilities, however the password needed for the administrative access has been revealed publicly.

No other Juniper Networks products or platforms are affected by these issues.

Juniper has issued a statement about these vulnerabilities at: <http://forums.juniper.net/t5/Security-Incident-Response/bg-p/SIRT>

SOLUTION:

The following software releases have been updated to resolve these specific issues: ScreenOS 6.2.0r19, 6.3.0r21, and all subsequent releases.

Additionally, earlier affected releases of ScreenOS 6.3.0 have been respun to resolve these issues. Fixes are included in: 6.3.0r12b, 6.3.0r13b, 6.3.0r14b, 6.3.0r15b, 6.3.0r16b, 6.3.0r17b, 6.3.0r18b, 6.3.0r19b.

All affected software releases on <http://www.juniper.net/support/downloads/screenos.html> have been updated with these fixes.

KB16765 - "In which releases are vulnerabilities fixed?" describes which release vulnerabilities are fixed as per our End of Engineering and End of Life support policies.

WORKAROUND:

The Juniper SIRT strongly recommends upgrading to a fixed release (in Solution section above) to resolve these critical vulnerabilities.

[CVE-2015-7755 \(unauthorized access\) Mitigation](#)

Restricting management access to only trusted management networks and hosts will help mitigate this issue. The attack can only be executed from a location where a legitimate management login would be permitted.

[CVE-2015-7756 \(VPN decryption\) Mitigation](#)

No workaround or detection exists for the VPN decryption vulnerability.

[Security Best Current Practice \(BCP\)](#)

In addition to the recommendations listed above, it is good security practice to limit the exploitable attack surface of critical infrastructure networking equipment. Use access lists or firewall filters to limit management access to the device only from

trusted, internal, administrative networks or hosts.

IMPLEMENTATION:

How to obtain fixed software:

ScreenOS software releases are available at <http://www.juniper.net/support/downloads/screensos.html>

MODIFICATION HISTORY:

2015-12-17: Initial publication
2015-12-17: Clarified that VPN decryption requires access to VPN traffic.
2015-12-18: Clearly separated two issues with two CVE IDs and two mitigation statements.
2015-12-20: Researcher revealed password for administrative access publicly.
2015-12-20: Added more specific affected versions for each issue.

RELATED LINKS:

[KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process](#)

[KB16765: In which releases are vulnerabilities fixed?](#)

[KB16446: Common Vulnerability Scoring System \(CVSS\) and Juniper's Security Advisories](#)

[Report a Vulnerability - How to Contact the Juniper Networks Security Incident Response Team](#)

[CVE-2015-7755: Unauthorized remote administrative access to ScreenOS](#)

[CVE-2015-7756: ScreenOS VPN decryption vulnerability](#)

[Juniper Networks Security Incident Response Team J-Net Blog](#)

CVSS SCORE:

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

RISK LEVEL:

Critical

RISK ASSESSMENT:

Information for how Juniper Networks uses CVSS can be found at KB 16446 "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

ACKNOWLEDGEMENTS:

[Site Map](#) / [RSS Feeds](#) / [Careers](#) / [Accessibility](#) / [Feedback](#) / [Privacy & Policy](#) / [Legal Notices](#)

Copyright© 1999-2012 Juniper Networks, Inc. All rights reserved.

J-Net Blogs Security Incident Response Important Announcement about ScreenOS®



Important Announcement about ScreenOS®

by [Derrick Scholl \(dscholl\)](#) 12-17-2015 09:02 AM - edited

IMPORTANT JUNIPER SECURITY ANNOUNCEMENT

CUSTOMER UPDATE: DECEMBER 20, 2015

Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through 6.3.0r20. VPN Decryption (CVE-2015-7756) only affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20.

We strongly recommend that all customers update their systems and apply these patched releases with the highest priority.

POSTED BY BOB WORRALL, SVP CHIEF INFORMATION OFFICER ON DECEMBER 17, 2015

Juniper is committed to maintaining the integrity and security of our products and wanted to make customers aware of critical patched releases we are issuing today to address vulnerabilities in devices running ScreenOS® software.

During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen® devices and to decrypt VPN connections. Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS.

At this time, we have not received any reports of these vulnerabilities being exploited; however, we strongly recommend that customers update their systems and apply the patched releases with the highest priority.

On behalf of the entire Juniper Security Response Team, please know that we take this matter very seriously and are making every effort to address these issues. More information and guidance on applying this update to systems can be found in the Juniper Security Advisories (JSAs) available on our Security Incident Response website at <http://advisory.juniper.net>.

Bob Worrall
SVP Chief Information Officer

Q: Why did this issue require an out-of-cycle security advisory?

Juniper is committed to maintaining the integrity and security of our products. Consistent with industry best practices, this means releasing patches for products in a timely manner to maintain customer security. We believed that it was in our customers' best interest to issue these patched releases with the highest priority.

We strongly recommend that all customers update their systems and apply these patched releases as soon as possible.

Q: What devices do these issues impact?

Administrative access (CVE-2015-7755) only affects devices running ScreenOS 6.3.0r17 through 6.3.0r20. VPN Decryption (CVE-2015-7756) only affects devices running ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20.

We strongly recommend that all customers update their systems and apply the patched releases with the highest priority

Q: Is the SRX or any other Junos®-based system affected by these issues?

These vulnerabilities are specific to ScreenOS. We have no evidence that the SRX or other devices running Junos are impacted at this time.

Q: Who can I contact if I have additional questions about my system?

Customers with questions about their systems should e-mail us at sirt@juniper.net