



KB & Security Advisory

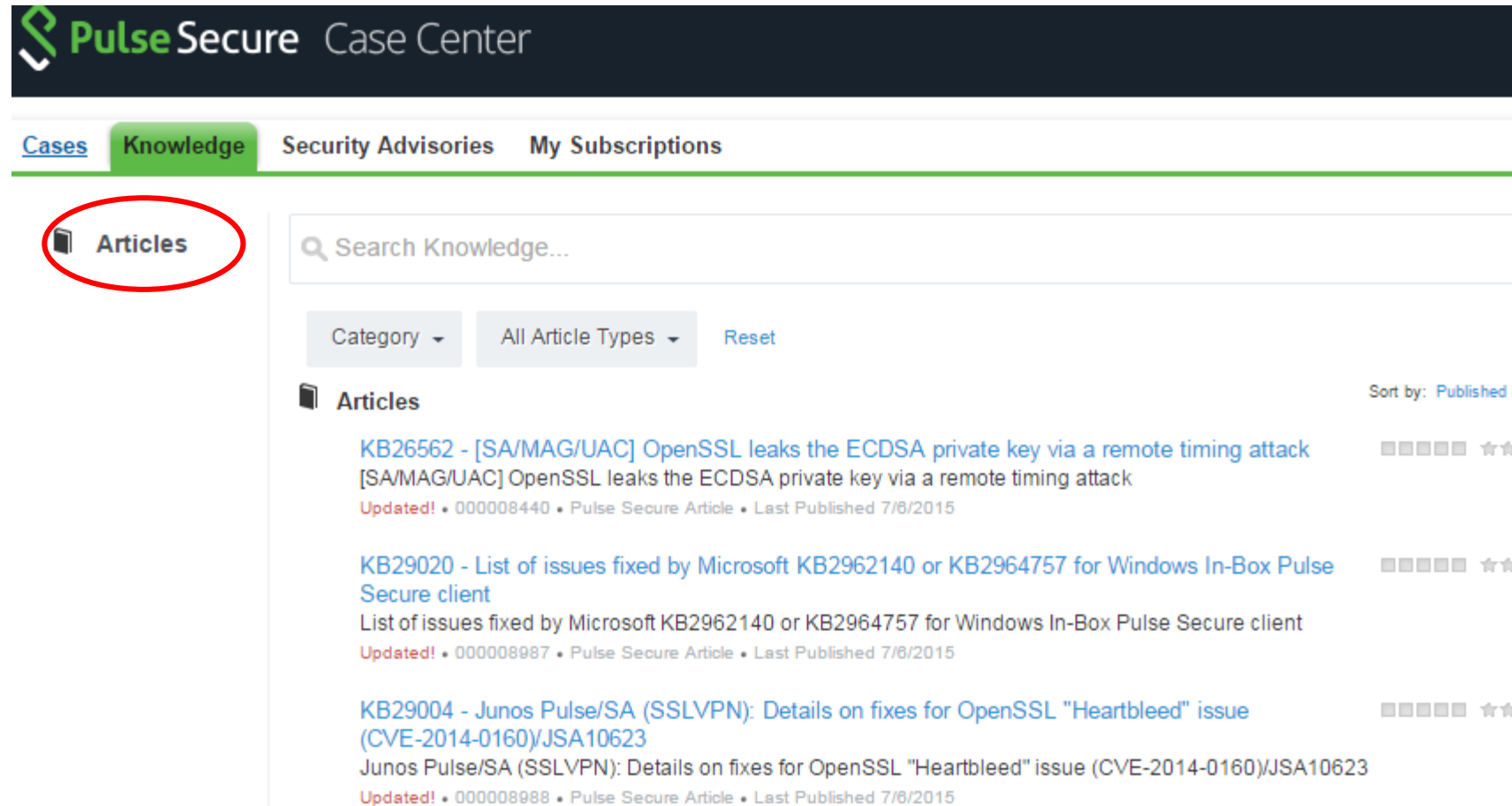
User Guide

The information contained herein is confidential and proprietary to Pulse Secure LLC and may not be disclosed without its permission. It is only intended to outline Pulse Secure's current "Roadmap" of its general product direction and is subject to change at any time without notice. The Roadmap is not a commitment, promise or legal obligation to deliver any material, code or functionality. It is for information purposes only and should not be relied upon in making any purchase decision or incorporated into any contract. It is provided "AS IS", without warranty of any kind, either express or implied. The development, release and timing of any features or functionality described for Pulse Secure products remains at the sole discretion of Pulse Secure. Any reliance upon the information contained herein shall be at the user's sole risk.

Searching Knowledge Articles

How to access knowledge articles

- Login to the Case Center
- Click the “Knowledge” tab



Pulse Secure Case Center

[Cases](#) **Knowledge** [Security Advisories](#) [My Subscriptions](#)

Articles

Search Knowledge...

Category ▾ All Article Types ▾ [Reset](#)

Articles Sort by: [Published Date](#)

- [KB26562 - \[SA/MAG/UAC\] OpenSSL leaks the ECDSA private key via a remote timing attack](#) ★★★★☆
[SA/MAG/UAC] OpenSSL leaks the ECDSA private key via a remote timing attack
Updated! • 000008440 • Pulse Secure Article • Last Published 7/8/2015
- [KB29020 - List of issues fixed by Microsoft KB2962140 or KB2964757 for Windows In-Box Pulse Secure client](#) ★★★★☆
List of issues fixed by Microsoft KB2962140 or KB2964757 for Windows In-Box Pulse Secure client
Updated! • 000008987 • Pulse Secure Article • Last Published 7/8/2015
- [KB29004 - Junos Pulse/SA \(SSLVPN\): Details on fixes for OpenSSL "Heartbleed" issue \(CVE-2014-0160\)/JSA10623](#) ★★★★☆
Junos Pulse/SA (SSLVPN): Details on fixes for OpenSSL "Heartbleed" issue (CVE-2014-0160)/JSA10623
Updated! • 000008988 • Pulse Secure Article • Last Published 7/8/2015

Search using Keywords

- Use keywords to search content.
- Results are displayed with the most relevant articles listed first.

The screenshot shows the Pulse Secure Knowledge base interface. At the top, there are navigation tabs: 'Cases', 'Knowledge' (highlighted in green), 'Security Advisories', and 'My Subscriptions'. Below the tabs, on the left, is a sidebar with 'Articles' and a search icon. The main search bar contains the text 'Heartbleed' and is circled in red. Below the search bar are filters for 'Category', 'All Article Types', and a 'Reset' button. To the right of the filters is a 'Sort by: Relevance' dropdown. The search results are listed under the heading 'Articles'. The first result is 'KB29004 - Junos Pulse/SA (SSLVPN): Details on fixes for OpenSSL "Heartbleed" issue (CVE-2014-0160)/JSA10623'. The second result is 'TSB16368 - Update: The Junos Pulse for iOS 5.0R3 Software Pre-Release Notification "Heartbleed" issue (CVE-2014-0160). For more information refer to JSA10623 ...'. The third result is 'KB29020 - List of issues fixed by Microsoft KB2962140 or KB2964757 for Windows In-Box Pulse Secure client'. Each result includes a title, a brief description, and a 'Updated!' status with a date.

Cases Knowledge Security Advisories My Subscriptions

Articles

Heartbleed

Category All Article Types Reset

Articles Sort by: Relevance

KB29004 - Junos Pulse/SA (SSLVPN): Details on fixes for OpenSSL "Heartbleed" issue (CVE-2014-0160)/JSA10623
Exposure to OpenSSL **Heartbleed** vulnerability described in JSA10623 ... Junos Pulse/SA (SSLVPN): Details on fixes for OpenSSL "**Heartbleed**" issue ... This article provides detailed information related to the fixes for OpenSSL "**Heartbleed**" issue ...
Updated! • 000008988 • Pulse Secure Article • Last Published 7/6/2015

TSB16368 - Update: The Junos Pulse for iOS 5.0R3 Software Pre-Release Notification "Heartbleed" issue (CVE-2014-0160). For more information refer to JSA10623 ...
000011131 • Pulse Technical Bulletin • Last Published 4/24/2015

KB29020 - List of issues fixed by Microsoft KB2962140 or KB2964757 for Windows In-Box Pulse Secure client
In-Box Pulse Secure client. Addresses the "**heartbleed**" security vulnerability (CVE-2014-0160 ...
Updated! • 000008987 • Pulse Secure Article • Last Published 7/6/2015

Search Filters

- Use filters to refine search results further.
- In the example below, articles related to Heartbleed would be returned for all product types and all article types.

The screenshot shows the Pulse Secure Knowledge base interface. The 'Knowledge' tab is selected. A search bar contains the text 'Heartbleed'. Below the search bar, there are two dropdown menus: 'Category' and 'All Article Types'. The 'All Article Types' dropdown is open, showing a list of filter options: 'No Filter' (selected), 'All', 'CONNECT-SECURE', 'SBR', 'WORKSPACE', 'MSS', and 'POLICY SECURE / OAC'. The search results are partially visible, showing article titles like 'SSLVPI 14-0160' and 'Heartbleed vuln'.

The screenshot shows the Pulse Secure Knowledge base interface. The 'Knowledge' tab is selected. A search bar contains the text 'Heartbleed'. Below the search bar, there are two dropdown menus: 'Category' and 'All Article Types', along with a 'Reset' button. The 'All Article Types' dropdown is open, showing a list of filter options: 'All Article Types', 'Pulse Bug Review', 'Pulse Secure Article', 'Pulse Security Advisory', 'Pulse Technical Bulletin', and 'Pulse Technote'. The search results are visible, showing article titles like 'KB29004 - Heartbleed', 'TSB16368 - Heartbleed', and 'KB29020 - Secure client'. The article descriptions mention 'Exposure to', 'on fixes for C', 'for OpenSSL', 'Updated!', '5.0R3 Software Pre-Release', and 'In-Box Pulse Secure client. Addresses the "heartbleed" security vulnerability (C)'.

Security Advisories

Searching Security Advisories

- Click on the Security Advisories Tab
- Enter a search phrase and related articles are returned in the query results with the key word from the search displayed in bold text.

Cases Knowledge **Security Advisories** My Subscriptions


cross site script


JSA10330 - NetScreen **Cross Site Scripting** Vulnerability, Released 03/01/04

JSA10402 - Secure Access (SA) and Unified Access Control (UAC) products - Multiple Web-based CGI and **Cross Site Scripting** (XSS) vulnerat

JSA10428 - 2010-03 Security Bulletin: Secure Access (SA) product - **Cross site scripting** issue on end user edit bookmarks page

JSA10444 - 2010-06 Security Bulletin: Secure Access (SA) & Unified Access Control (UAC): **Cross Site Scripting** Issue during Signout

 JSA10445 - 2010-06 Security Bulletin: Secure Access (SA) **Cross Site Scripting** Issue in Windows Secure Application Manager
2013-09 Security Bulletin: Junos Pulse Secure Access Service (IVE) and Junos Pulse Access Control Service (UAC): Crafted packet can cause denial of service

 [JSA10617 - 2014-03 Security Bulletin: Junos Pulse Secure Access Service \(SSL VPN\): Cross site scripting issue \(CVE-2014-2291\)](#)
2014-03 Security Bulletin: Junos Pulse Secure Access Service (SSL VPN): Cross site scripting issue (CVE-2014-2291)

Subscribing for Updates

- Selecting an article will open the article details in a new window.
- To receive future updates for a specific article, click “Subscribe” at the bottom of the page.

Solution The following IVE software releases have a fix for these issues, SA (IVE): 6.5R10; 7.0R7, 7.1R4 or higher. We recommend upgrading your IVE software to resolve this security vulnerability.

Note: Juniper Networks policy is to only publish fixes for release that have not yet reached End-of-Engineering. These issues were reported prior to date so the fixes for this release are published in this Security Bulletin.

Information regarding the Juniper Network fix policy for Security Issues can be found at KB16765 "In which releases are vulnerabilities fixed?"

Workaround None.

Implementation

Related Links [IVE Software Download URL](#)
[KB 16765 - In which releases are vulnerabilities fixed?](#)
[KB 16613 - Juniper SIRT's Regularly-Scheduled Security Bulletin Publication Process](#)

Risk Assessment - You can gain unauthorized access to protected resources.

Acknowledgements

Risk Level Medium

Attachment 1

Attachment 2

Document ID JSA10490

Subscribe

Managing Subscriptions

- All subscriptions are maintained in “My Subscriptions”.
- Select the tab “My Subscriptions” to view current subscriptions.
- Click “Unsubscribe” to stop receiving updates for any given subscription.

Cases Knowledge Security Advisories **My Subscriptions**

Source Subscriptions	Options
Security Advisories	Unsubscribe

Content Subscriptions	Options
JSA10470 - Pre-authentication CGI script fails to fully validate all parameters	Unsubscribe
JSA10490 - 2011-09 Security Bulletin: Secure Access (SA): Cross Site Scripting Issues	Unsubscribe
JSA10592 - 2013-09: Security, Access, and Acceleration: Security Advisories Released	Unsubscribe



Thank you

The information contained herein is confidential and proprietary to Pulse Secure LLC and may not be disclosed without its permission. It is only intended to outline Pulse Secure's current "Roadmap" of its general product direction and is subject to change at any time without notice. The Roadmap is not a commitment, promise or legal obligation to deliver any material, code or functionality. It is for information purposes only and should not be relied upon in making any purchase decision or incorporated into any contract. It is provided "AS IS", without warranty of any kind, either express or implied. The development, release and timing of any features or functionality described for Pulse Secure products remains at the sole discretion of Pulse Secure. Any reliance upon the information contained herein shall be at the user's sole risk.