Cisco Policy Suite Software Version 13.1.0 Patch Release Notes

First Published: February 07, 2018
Last Updated: February 07, 2018

Introduction

This release note identifies issues resolved and any enhancements made in this patch release for Cisco Policy Suite (CPS) software version 13.1.0.

Patch Details

The following table lists the patch details.

Patch Information	Details
Patch Name	CPS_Hotfix_Patch1_13.1.0.tar.gz
Patch Download Link	https://software.cisco.com/download/release.html?i=!y&mdfid=284883911&softwareid=284979976&release=13.1.0&os
Md5sum	db14dd9047b92c16abc4f263b5c617b0

The following table lists the component version details for this patch release.

Component	Version
Core	13.1.1.r113649

Patch Installation

To install this patch:

Note: Patches must be applied during a maintenance window.

1. Log on to the Cluster Manager as root user.
2. Download the patch file to the Cluster Manager VM.

See the Patch Details section for download information.

3. Run the patch -a command to apply the patch.

```
/var/qps/install/current/scripts/patch/patch –a /tmp/CPS_Hotfix_Patch1_13.1.0.tar.gz
```

4. Run the following command to restore the Policy Builder configurations.

```
/var/qps/install/current/scripts/setup/restorePolicyRepositories.sh
```

5. Run build_all.sh script to create updated CPS packages. This builds updated VM images on the Cluster Manager with the new patch applied.

```
/var/qps/install/current/scripts/build_all.sh
```

6. Update the VMs with the new software using reinit.sh script. This triggers each CPS VM to download and install the updated VM images from the Cluster Manager.

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

7. Restart all software components on target VMs by running the script.

```
restartall.sh
```

8. Run about.sh to verify that the component is updated.

```
Example:

 [root@lab tmp]# about.sh

Cisco Policy Suite - Copyright (c) 2015. All rights reserved.

CPS AIO

CPS Installer Version - 13.1.0

CPS Core Versions

---------------------------

   lab: qns-1      (pcrf): 13.1.1.r113649

   lab: qns-2        (pb): 13.1.1.r113649

CPS Patch History

---------------------------

CPS_Hotfix_Patch1_13.1.0 - February 07 2018 10:42:11.
```

Patch Rollback

This section describes how to roll back this patch if a patching failure occurs.

To roll back this patch:

1. Log on to the Cluster Manager as root user.
2. To undo the applied patch, execute the following command on the Cluster Manager.

```
/var/qps/install/current/scripts/patch/patch –u CPS_Hotfix_Patch1_13.1.0
```

3. To completely remove a patch and all related items from the Cluster Manager.

   ```
   /var/qps/install/current/scripts/patch/patch -r CPS_Hotfix_Patch1_13.1.0
   ```

   This deletes the patch file from the /var/qps/.tmp/patches directory of the Cluster Manager

4. After undoing/removing the applied patch execute the following commands in Cluster Manager to re-build the CPS system and push the changes to VMs.

   ```
   /var/qps/install/current/scripts/build_all.sh
   ```

   ```
   /var/qps/install/current/scripts/upgrade/reinit.sh
   ```

5. Restart all software components on target VMs by running the script.

   ```
   restartall.sh
   ```

Issues Resolved in this Patch Release

This section identifies issues that have been resolved in this patch release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

CSCvg40124: Cisco Policy Suite Radius Authentication Bypass Vulnerability

CSCvg47830: Cisco Policy Suite Radius Authentication Information Disclosure Vulnerability

For further information regarding these vulnerabilities, please refer to the Cisco Security Advisories:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps1

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks

mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)