Patch Assessment Content Update Release Notes for CCS 12.x

Version: 2019-4 Update

Symantec

Patch Assessment Content Update Release Notes for CCS 12.x

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Patch Assessment Content Update (PACU)

This document includes the following topics:

Prerequisites for PACU

Following are the prerequisites for installing the Patch Assessment Content Updates:

- **Symantec Control Compliance Suite 12.x**
  Before you install a Patch Assessment Content Update, you must have the Control Compliance Suite 12.x installed on your computer.
- **Security Content Updates (SCU) 2018-3**
  To install PACU 2019-1 or later, you must have the Security Content Update 2018-3 installed on your computer.
- **New signing certificate**
  A new signing certificate is used for all CCS files that are signed after March 03, 2019. To install PACU 2019-3 or later by using the LiveUpdate feature, you need this certificate. The certificate is valid till March 03, 2020. For the updated certificate, you must apply the Quick Fix (QF) 10142 for CCS 12.0 or 12.0.1 and Quick Fix (QF) 10002 for CCS 12.5. These QFs include the Symantec.CSM.AssemblyVerifier.dll, which contains the updated CCS

certificate information necessary to validate the certificate. You can download the .zip package for these QFs from the following location:
http://www.symantec.com/docs/TECH228300

Note: If the QF 10142 for CCS 12.0 or 12.0.1 and Quick Fix (QF) 10002 for CCS 12.5 is not applied, the Automatic Updates Installation job will fail. However, there is no impact on the manual installation of PACU without this QF.

What's New in PACU 2019-4

PACU 2019-4 contains the following updates:

- Security Updates and Quality Updates for Windows
  See "Security Updates and Quality Updates for Windows" on page 6.
- Security Updates for UNIX
  See "Security Updates for UNIX" on page 8.

Note: The **Oracle Patch Assessment Standard** is available in Control Compliance Suite 12.0 from PACU 2018-2 onwards. For detailed information about this standard, refer to the Patch Assessment Content Update Getting Started Guide for Control Compliance Suite 12.0.

See "Contents of PACU" on page 8.

Security Updates and Quality Updates for Windows

PACU 2019-4 contains the updated Windows Patch Assessment Standard. This standard comprises checks related to security update rollups and quality update rollups that are released by Microsoft in April 2019 for raw-data content.

Table 1-1 contains the following information about the new security update rollups released by Microsoft in April 2019:

- Name of the update rollup
- Maximum severity rating for the rollup
- Links to the Microsoft Knowledge Base (KB) articles for more information about the respective update rollups

Note: PACU 2019-4 includes Operating System related update rollups.

Table 1-1 Microsoft Update Rollups in PACU 2019-4

Update Rollup	Severity Rating	KB Article
April 9, 2019—KB4493450 (Security-only update)	Critical	KB4493450
April 9, 2019—KB4493458 (Security-only update)	Critical	KB4493458
April 9, 2019—KB4493448 (Security-only update)	Critical	KB4493448
April 9, 2019—KB4493467 (Security-only update)	Critical	KB4493467
April 9, 2019—KB4493451 (Monthly Rollup)	Critical	KB4493451
April 9, 2019—KB4493472 (Monthly Rollup)	Critical	KB4493472
April 9, 2019—KB4493446 (Monthly Rollup)	Critical	KB4493446
April 9, 2019—KB4493471 (Monthly Rollup)	Critical	KB4493471
April 2, 2019—KB4490481 (OS Build 17763.404)	Critical	KB4490481
March 19, 2019—KB4489889 (OS Build 14393.2879)	Critical	KB4489889
April 9, 2019—KB4493475 (OS Build 10240.18186)	Critical	KB4493475
April 9, 2019—KB4493474 (OS Build 15063.1747)	Critical	KB4493474
March 19, 2019—KB4489894 (OS Build 17134.677)	Critical	KB4489894
March 19, 2019—KB4489890 (OS Build 16299.1059)	Critical	KB4489890
March 19, 2019—KB4489888 (OS Build 15063.1716)	Critical	KB4489888
April 9, 2019—KB4493464 (OS Build 17134.706)	Critical	KB4493464
April 9, 2019—KB4493470 (OS Build 14393.2906)	Critical	KB4493470
April 9, 2019—KB4493509 (OS Build 17763.437)	Critical	KB4493509
April 9, 2019—KB4493441 (OS Build 16299.1087)	Critical	KB4493441

Note: Severity ratings of security bulletins are decided by Microsoft and are intended to help customers assess security vulnerabilities in their environments. However, we recommend that customers evaluate their CCS environments and decide which Microsoft updates need to be applied and their deployment priorities.

See "Contents of PACU" on page 8.

Security Updates for UNIX

The updated patches and the new patches in .dat (template) files are available for raw-data content on UNIX platforms.

Security updates for the following UNIX platforms are available in this release:

- Red Hat Enterprise Linux
- Ubuntu

See "Contents of PACU" on page 8.

Contents of PACU

PACU contains the following files:

Table 1-2 Contents of PACU

Name	Description
WindowsPatchCheckStandard.xml	Raw-data content standard for Windows
OraclePatchAssesssment.xml	Raw-data content standard for Oracle databases
OraclePatchAssesssment_Command.xml	Command file for Oracle Patch Assessment Standard
OracleDBRecommendedPatches.dat	Raw-data content updates for Oracle databases
LinuxRecommendedPatches.dat	Raw-data content updates for Linux platforms
HP-UXRecommendedPatches.dat	Raw-data content updates for HP-UX platforms
AIXRecommendedPatches.dat	Raw-data content updates for AIX platforms
SunOSRecommendedPatches.dat	Raw-data content updates for Sun OS platforms
UbuntuRecommendedPatches.dat	Raw-data content updates for Ubuntu platforms
ESM_OSPatches_Comprehensive.xml	Message-based content updates for Windows and UNIX
BestPractice_OS_Patch_Updates.exe	Patch Policy updates on message- based content for Windows and UNIX.
Comprehensive_AIXPatchStandard.xml	Contains checks which evaluate on APAR and Packages for AIX OS

Table 1-2 Contents of PACU *(continued)*

Name	Description
Symantec.CSM. UnixPlatformContent.UnixPatchStandard.dll Version 12.0.10000.1300	Custom algorithm used for evaluating package checks in the Comprehensive Patch Standard for AIX.
WindowsPatchData.zip	Raw-data content file for Windows data collection