Avocent® ACS 6000 Advanced Console Server
Release Notes UPDATE!
Version 3.3.0.12
January 13, 2017

This document outlines:

1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug Fixes

==========

1. Update Instructions

==========

NOTE: Please refer to the ACS 6000 Installer/User Guide for detailed instructions on updating the ACS 6000 console server to version 3.3.0.

IMPORTANT NOTE: This version should be upgraded from version 2.5.0.11 or newer. Appliances with earlier versions should be upgraded to version 2.5.0.11 before the upgrade to version 3.3.0.

In order to have all features listed in this release available through the Avocent® DSView™ management software, DSView™ software version 4.5 (SP5 or later) and ACS 6000 console server plug-in version 3.3.0 are required.

When applicable, after the ACS 6000 console server firmware has been upgraded to version 3.3.0, it is mandatory that the web browser cache of any system which intends to be connected to the ACS 6000 console server web interface is cleared. To do this, press **Ctrl-F5** from the browser.

ACS 6000 console server firmware version 3.3.0 provides an internal mechanism which preserves the existing configuration when upgrading from previous firmware versions. However, it is strongly recommended that you back up the system configuration before firmware version upgrades.

==========

2. Appliance Firmware Version Information

==========

The following languages are supported by ACS 6000 console server version 3.3.0.12:

- English
- Japanese
- Simplified Chinese

NOTE: As listed in the following table, the firmware download is a .zip file which must be extracted before use.

Appliance/Product	Firmware Type	Version	Filename
Avocent® ACS 6000 Console Server	Opcode	3.3.0.12	avoImage_avctacs-3.3.0.12.zip avoImage_avctacs-3.3.0.12.zip.md5

==========

3. Features/Enhancements

==========

NOTE: Please refer to the ACS 6000 Installer/User Guide and/or Command Reference Guide for details about features supported by the ACS 6000 console server version 3.3.0.

Client Browser Support Information

- Microsoft® Internet Explorer® 9, 10, and 11.
- Mozilla® Firefox® version 36.0.1 in Windows 7.

==========

4. Bug Fixes

==========

The following table lists the bug/patch fixes included in version 3.3.0.12.

Issue Number	Additional Information	Description
L3-487234-614476945	ACS 6000 [console server] Error: *Could not get Session ID*.	This patch fix address the L3 case reporting that a customer's SSH scripts are failing and show intermittent *Could not get Session ID* errors. The fix prevents orphaned SSH sessions. The root-cause has to do with the SSH process exiting prematurely before its associated session is destroyed.
L3-487234-651527965	(CVE-2016-5195), dirtyCOW vulnerability	This patch fix addresses the L3 case reporting the dirtyCOW vulnerability (CVE-2016-5195) caused by a race condition found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.