**Product Correction Notice (PCN)**

| | |
|---|---|
| **Issue Date:** | **08-May-2017** |
| **Supplement Date:** | **11-January-2021** |
| **Expiration Date:** | **NA** |
| **PCN Number:** | **2065S** |

**SECTION 1 - CUSTOMER NOTICE**

**Products affected by this PCN:**

Avaya Aura® Utility Services 7.1.x, all offers.

**Description:**

**11-Jan-2021** Supplement 14 of this PCN introduces Service Pack 7.1.3.8 for Avaya Aura® Utility Services. Service Pack 7.1.3.8 should be applied to all Utility Services 7.1.x Virtual Machines either from the Command Line Interface (CLI) or from Solution Deployment Manager (SDM). A manual reboot after the service pack installation is necessary to activate the patch.

For systems running AVP, the Utility Services software specified in this PCN was verified and is compatible with AVP release 7.1.3.8.0.05. See PCN 2064S for more information. AVP must be upgraded to the compatible release before upgrading Utility Services.

This is the final Service Pack for Aura 7.x. Customers should actively plan to upgrade to a supported load.

**Service Pack 7.1.3.8 (util_patch_7.1.3.8.0.05.zip, PLDS ID US000000097)**
Reference the Avaya Aura 7.1.3.x Release Notes for non-security related fixes delivered to 7.1.3.7

RHSA-2020:5437-01 Important: kernel security and bug fix update
RHSA-2020:4276: Important: kernel security update
RHSA-2020-4005: Important/Sec libxslt security update
RHSA-2020-3901: Important/Sec libpng security update
RHSA-2020:4350: Important/Sec java-1.8.0-openjdk
RHSA-2020:3971: Moderate/Sec hunspell
RHSA-2020:5023: Important/Sec kernel
RHSA-2020:5009: Low/Sec python
RHSA-2020:5083: Important/Sec microcode_ctl
RHSA-2020:3864: Moderate /Sec cups
RHSA-2020:4908: Low/Sec libX11
RHSA-2020:5011: Important/Sec bind
RHSA-2020:5002: Moderate/Sec curl
RHSA-2020:3878: Important/Sec dnsmasq
RHSA-2020:4907: Important/Sec freetype
RHSA-2020:4041: Important/Sec openldap
RHSA-2020:2432: Important/Sec microcode_ctl
CVE-2020-8177: Important/Sec Red Hat curl local file overwrites
Important/Sec Apache Tomcat 7.0.x lt 7.0.105 WebSocket DoS (tcp)
Security issue with sms_test.php
SMS rpm from AES for AES-16068 where UTF8 native name improperly handled

**9-Nov-2020** Supplement 13 of this PCN introduces Service Pack 7.1.3.7 for Avaya Aura® Utility Services. Service Pack 7.1.3.7 should be applied to all Utility Services 7.1.x Virtual Machines either from the Command Line Interface (CLI) or from Solution Deployment Manager (SDM). A manual reboot after the service pack installation is necessary to activate the patch.

For systems running AVP, the Utility Services software specified in this PCN was verified and is compatible with AVP release 7.1.3.7.0.04. See PCN 2064S for more information. AVP must be upgraded to the compatible release before upgrading Utility Services.

**Service Pack 7.1.3.7 (util_patch_7.1.3.7.0.03.zip, PLDS ID US000000096)**
Reference the Avaya Aura 7.1.3.x Release Notes for non-security related fixes delivered to 7.1.3.7

Removed deprecated SSH Cryptographic Settings
Removed weak ciphers from TLS provided cipher suite
Addressed XSS vulnerability (cross site scripting)
HTTPS server is not enforcing HTTP Strict Transport Security (HSTS).
CVE-2004-1653 - UtilServ should disable ssh AllowTCPForwarding
CVE-2020-9484 Important/Sec Apache Tomcat Remote Code Execution via session persistence
CVE-2020-11996 A specially crafted sequence of HTTP/2 requests could trigger high CPU usage for several seconds per ASA-2020-097
CVE-2020-13935 Important: WebSocket DoS Vulnearability
RHSA-2020:4076 Important/Sec nss and nspr
RHSA-2020:4072 Important/Sec libcroco
RHSA-2020:4060 Important/Sec kernel
RHSA-2020:4032 Important/Sec dbus
RHSA-2020:4026 Important/Sec mariadb
RHSA-2020:4011 Important/Sec e2fsprogs
RHSA-2020:4007 Important/Sec systemd
RHSA-2020:4003 Important/Sec NetworkManager
RHSA-2020:3996 Important/Sec libxml2
RHSA-2020:3978 Important/Sec glib2 and ibus
RHSA-2020:3958 Important/Sec httpd
RHSA-2020:3952 Important/Sec expat
RHSA-2020:3916 Important/Sec curl
RHSA-2020:3915 Important/Sec libssh2
RHSA-2020:3908 Important/Sec cpio
RHSA-2020:3902 Important/Sec libtiff
RHSA-2020:3861 Important/Sec glibc
RHSA-2020:3276 Important/Sec grub2
RHSA-2020:3217 Important/Sec grub2
RHSA-2020:2968 Important/Sec java-1.8.0-openjdk
RHSA-2020:2894 Important/Sec dbus
RHSA-2020:2832 Important/Sec kernel
RHSA-2020:2664 Important/Sec kernel
RHSA-2020:2663 Important/Sec ntp
RHSA-2020:2642 Important/Sec unbound
RHSA-2020:2432 Important/Sec microcode_ctl
RHSA-2020-2344 Important/Sec bind security update Reference ASA-2020-079
RHSA-2020-2082 Important/Sec reference ASA-2020-075 kernel update and bug fixes

RHSA-2020:1512 Important/Sec. java-1.8.0-openjdk-1:1.8.0.252.b09-2.el7_8.x86_64
RHSA-2020:1190 Moderate/Sec. libxml2-2.9.1-6.el7.4.x86_64
RHSA-2020:1181 Low/Sec. unzip-6.0-21.el7.x86_64
RHSA-2020:1180 Moderate/Sec. emacs-filesystem-1:24.3-23.el7.noarch
RHSA-2020:1180 Important/Sec ImageMagick
RHSA-2020:1176 Low/Sec. avahi-libs-0.6.31-20.el7.x86_64
RHSA-2020:1138 Low/Sec. gettext-0.19.8.1-3.el7.x86_64
RHSA-2020:1135 Low/Sec. polkit-0.112-26.el7.x86_64
RHSA-2020:1131 Moderate/Sec. python-2.7.5-88.el7.x86_64
RHSA-2020:1121 Moderate/Sec. httpd-2.4.6-93.el7.x86_64
RHSA-2020:1113 Moderate/Sec. bash-4.2.46-34.el7.x86_64
RHSA-2020:1112 Moderate/Sec. php-5.4.16-48.el7.x86_64
RHSA-2020:1100 Moderate/Sec. mariadb-libs-1:5.5.65-1.el7.x86_64
RHSA-2020:1080 Moderate/Sec. atk-2.28.1-2.el7.x86_64
RHSA-2020:1061 Moderate/Sec. bind-32:9.11.4-16.P2.el7.x86_64
RHSA-2020:1050 Moderate/Sec. cups-libs-1:1.6.3-43.el7.x86_64
RHSA-2020:1022 Low/Sec. file-5.11-36.el7.x86_64
RHSA-2020:1021 Moderate/Sec. gsettings-desktop-schemas-3.28.0-3.el7.x86_64
RHSA-2020:1020 Low/Sec. curl-7.29.0-57.el7.x86_64
RHSA-2020:1016 Moderate/Sec. kernel-3.10.0-1127.el7.x86_64
RHSA-2020:1011 Moderate/Sec. expat-2.1.0-11.el7.x86_64
RHSA-2020:1000 Moderate/Sec. rsyslog-8.24.0-52.el7.x86_64

**13-Apr-2020** Supplement 12 of this PCN introduces Service Pack 7.1.3.6 for Avaya Aura® Utility Services. Service Pack 7.1.3.6 should be applied to all Utility Services 7.1.x Virtual Machines either from the Command Line Interface (CLI) or from Solution Deployment Manager (SDM). A manual reboot after the service pack installation is necessary to activate the patch.

For systems running AVP, the Utility Services software specified in this PCN was verified and is compatible with AVP release 7.1.3.6.0.02. See PCN 2064S for more information. AVP must be upgraded to the compatible release before upgrading Utility Services.

**Service Pack 7.1.3.6 (util_patch_7.1.3.6.0.03.zip, PLDS ID US000000095)**
Reference the Avaya Aura 7.1.3.x Release Notes for non-security related fixes delivered to 7.1.3.6.

This Service Pack provides the following security updates and fixes:
RHSA-2019-2600: kernel security and bug fix update
RHSA-2019:3834: Important: kernel security update
RHSA-2019:3872: Important: kernel security update
RHSA-2019:3976: Low: tcpdump security update
RHSA-2019:4190: Important: nss, nss-softokn, nss-util security update
RHSA-2019:3979: Important: kernel security and bug fix update
RHSA-2019:4254-01: Moderate: freetype security update
RHSA-2020:0196 java update
RHSA-2020:0227: sqlite update
RHSA-2020:0374: kernel update
RHSA-2020:0540: sudo update
RHSA-2020:0630: Important/Sec. ppp-2.4.5-34.el7_7.x86_64
RHSA-2020:0834: Important/Sec. kernel-3.10.0-1062.18.1.el7.x86_64
RHSA-2020:0897: Important/Sec. libicu-50.2-4.el7_7.x86_64

Tomcat Moderate: Local Privilege Escalation CVE-2019-12418, CVE-2019-17563 and CVE-2019-0221
Tomcat High: AJP Request Injection and potential Remote Code Execution CVE-2020-1938 HTTP Request Smuggling CVE-2020-1935 CVE-2019-17569

**04-Apr-2020** Supplement 11 of this PCN introduces updated Utility Services 7.1 OVA to address the expiration of the Avaya signing certificate used for Avaya Aura® OVAs.
Reference PSN020463u - Avaya Aura® OVA Certificate Expiry.
The PLDS download IDs will be the same, but the OVAs are updated.
No changes to software or functionality have occurred in these new OVAs.
The certificate and the signature file are renewed in the new OVAs.
The OVA file name has changed to reflect a new version number and the checksum is updated.

**VMware**
Utility Services 7.1 OVA (US-7.1.0.0.0.18-e55-3_OVF10.ova, **PLDS ID** US000000077)

**December 20th, 2019 –** Supplement 10 of this PCN introduces Service Pack 7.1.3.5 for Avaya Aura® Utility Services. Service Pack 7.1.3.5 should be applied to all Utility Services 7.1.x Virtual Machines either from the Command Line Interface (CLI) or from Solution Deployment Manager (SDM). A manual reboot after the service pack installation is necessary to activate the patch.

For systems running AVP, the Utility Services software specified in this PCN was verified and is compatible with AVP release 7.1.3.5.0.08. See PCN 2064S for more information. AVP must be upgraded to the compatible release before upgrading Utility Services.

**Service Pack 7.1.3.5 (util_patch_7.1.3.5.0.02.zip, PLDS ID US000000094)**
Reference the Avaya Aura 7.1.3.x Release Notes for non-security related fixes delivered to 7.1.3.5.

This Service Pack provides the following security updates and fixes:
RHSA-2019:3286 Critical/Sec. php-5.4.16-46.1.el7_7.x86_64
RHSA-2019:3197 Important/Sec. sudo-1.8.23-4.el7_7.1.x86_64
RHSA-2019:3128 Important/Sec. java-1.8.0-openjdk-1:1.8.0.232.b09-0.el7_7.x86_64
RHSA-2019:3197 Important: sudo security update
RHSA-2019:3055 Important: kernel security and bug fix update
RHSA-2019:3055 Important/Sec. kernel-3.10.0-1062.4.1.el7.x86_64
RHSA-2019:2829 Important/Sec. kernel-3.10.0-1062.1.2.el7.x86_64
RHSA-2019:2169 Important/Sec. linux-firmware-20190429-72.gitddde598.el7.noarch
RHSA-2019:2571 Important/Sec. pango-1.42.4-4.el7_7.x86_64
RHSA-2019:1619 Important/Sec. RHEL 7 / 8 : vim (RHSA-2019:1619)
RHSA-2019:1947 Important/Sec. vim-common-2:7.4.160-2.el7_4.1.x86_64
RHSA-2019:1587 Important/Sec. python.x86_64
RHSA-2019:2343 Moderate/Sec. httpd-2.4.6-90.el7.x86_64
RHSA-2019:2327 Moderate/Sec. mariadb-libs-1:5.5.64-1.el7.x86_64
RHSA-2019:2304 Moderate/Sec. openssl-1:1.0.2k-19.el7.x86_64
RHSA-2019:2272 Moderate/Sec. python-urllib3-1.10.2-7.el7.noarch
RHSA-2019:2237 Moderate/Sec. nspr-4.21.0-1.el7.x86_64
RHSA-2019:2189 Moderate/Sec. procps-ng-3.3.10-26.el7.x86_64
RHSA-2019:2177 Moderate/Sec. libsss_idmap-1.16.4-21.el7.x86_64
RHSA-2019:2136 Moderate/Sec. libssh2-1.8.0-3.el7.i686
RHSA-2019:2118 Moderate/Sec. glibc-2.17-292.el7.i686

RHSA-2019:2110 Moderate/Sec. rsyslog-8.24.0-38.el7.x86_64
RHSA-2019:2091 Moderate/Sec. libgudev1-219-67.el7.x86_64
RHSA-2019:2079 Moderate/Sec. libX11-1.6.7-2.el7.x86_64
RHSA-2019:2075 Moderate/Sec. binutils-2.27-41.base.el7.x86_64
RHSA-2019:2060 Moderate/Sec. dhclient-12:4.2.5-77.el7.x86_64
RHSA-2019:2057 Moderate/Sec. bind-32:9.11.4-9.P2.el7.x86_64
RHSA-2019:2053 Moderate/Sec. libtiff-4.0.3-32.el7.x86_64
RHSA-2019:2052 Moderate/Sec. libjpeg-turbo-1.2.90-8.el7.x86_64
RHSA-2019:2049 Moderate/Sec. libmspack-0.5-0.7.alpha.el7.x86_64
RHSA-2019:2047 Moderate/Sec. libcgroup-0.41-21.el7.x86_64
RHSA-2019:2046 Moderate/Sec. polkit-0.112-22.el7.x86_64
RHSA-2019:2030 Moderate/Sec. python-2.7.5-86.el7.x86_64
RHSA-2019:1884 Moderate/Sec. libssh2-1.4.3-12.el7_6.3.i686
RHSA-2019:1815 Moderate/Sec. java-1.8.0-openjdk-1:1.8.0.222.b10-0.el7_6.x86_64
RHSA-2019:2197 Low/Sec. elfutils-0.176-2.el7.x86_64
RHSA-2019:2181 Low/Sec. curl-7.29.0-54.el7.x86_64
RHSA-2019:2162 Low/Sec. blktrace-1.0.5-9.el7.x86_64
RHSA-2019:2159 Low/Sec. unzip-6.0-20.el7.x86_64
RHSA-2019:2143 Low/Sec. openssh-7.4p1-21.el7.x86_64
RHSA-2019:2077 Low/Sec. ntp-4.2.6p5-29.el7.x86_64
RHSA-2019:2035 Low/Sec. python-requests-2.6.0-5.el7.noarch
RHSA-2019-1815 OpenJDK: security issue

Custom login banner was not shown on web login home page

**July 8th, 2019 –** Supplement 9 of this PCN introduces Service Pack 7.1.3.4 for Utility Services, which is applicable to all hypervisor type supported version of Avaya Aura® Utility Services 7.1 – i.e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Service Pack 7.1.3.4 should be applied to all Utility Services 7.1 Virtual Machines either from cli of from SDM. A manual reboot post upgradation is necessary to activate the patch.

**Service Pack 7.1.3.4 (util_patch_7.1.3.4.0.05.zip, PLDS ID US000000093)**

This Service Pack addresses the following security updates and issue fixes:
[CVE-2019-0221] Apache Tomcat XSS in SSI printenv
[RHSA-2019:1228-01] Important: wget security update
[RHSA-2019:1481] Kernel update for RHEL7
[RHSA-2019:1294] [MEDIUM] RHEL 7: bind update
[RHSA-2019:1168] [HIGH] RHEL 7: kernel
Security vulnerability apache banner reveals information
[RHSA-2018-0849] gcc security, bug fix, and enhancement update
[RHSA-2018:0094] update kernel (linux firmware) for RHEL7
[RHSA-2018:0093] 106088 - RHEL 6 / 7: microcode_ctl (Spectre)
[RHSA-2019:0818] Update kernel for RHEL7
SSHD configuration enhanced to support ciphers prescribed by NIST
[RHSA-2019:0818-01] Important: kernel security and bug fix update
[RHSA-2019:0485-01] Moderate: tomcat security update
[RHSA-2019:0679-01] Important: libssh2 security update
[RHSA-2019:0710-01] Important: python security update

[RHSA-2019:0483-01] Moderate: openssl security and bug fix update
[RHSA-2019:0512-01] Important: kernel security, bug fix, and enhancement update
[RHSA-2019:0201] [LOW] RHEL 7: systemd update
[RHSA-2019:0368] [MEDIUM] RHEL 7: systemd update
[RHSA-2019:0230] [Medium] - RHEL 7: polkit update
[RHSA-2019:0163] [MEDIUM] RHEL 7: kernel update
[RHSA-2019:0435] [MEDIUM] RHEL 7: java-1.8.0-openjdk update
[RHSA-2019:0049] [HIGH] RHEL 7: systemd update
[RHSA-2019:0194] [MEDIUM] RHEL 7: bind update
[RHSA-2019:0109] [HIGH] RHEL 7: perl update
Unwanted wireless packages observed on the system
Privileged escalation possible with sudoers
Admin web page upload files allowed for remote command execution

**Feb-11th, 2019 –** Supplement 8 of this PCN introduces Service Pack 7.1.3.3 for Utility Services , which is applicable to all hypervisor type supported version of Avaya Aura® Utility Services 7.1 – i.e. e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Service Pack 7.1.3.3 should be applied to all Utility Services 7.1 Virtual Machines either from cli of from SDM. A manual reboot post upgradation is necessary to activate the patch.
This service pack introduces support for the Avaya Converged Platform (ACP) servers (ACP 120 and ACP 130) based on the Dell® PowerEdge R640.
**Service Pack 7.1.3.3 (util_patch_7.1.3.3.0.03.zip, PLDS ID US000000092)**

This Service Pack addresses the following security updates and issue fixes:
High: Privilege escalation possible with sudoers from SMI user
Important: Update tzdata to tzdata-2018g
[RHSA-2018:2748-01] Important: kernel security and bug fix update
[RHSA-2018:3083] Important: RHEL 7 : kernel security update
[RHSA-2018:3050] Medium: RHEL 7 : gnutls security update
[RHSA-2018:3059] Medium: RHEL 7 : X.org X11 security update
[RHSA-2018:3327] Low: RHEL 7 : libmspack security update
[RHSA-2018:2942] Low: RHEL 7 : java-1.8.0-openjdk security update
[RHSA-2018:2943] Important: RHEL 7 : java-1.8.0-openjdk security update
[RHSA-2018:3041] Important: RHEL 7 : python security update
[RHSA-2018:3249] Low: RHEL 7 : setup security update
[RHSA-2018:3032] Low: RHEL 7 : binutils security update
[RHSA-2018:3158] Medium: RHEL 7 : sssd security update
[RHSA-2018:3221] Low: RHEL 7 : openssl security update
[RHSA-2018:3092] Important: RHEL 7 : glibc security update
[RHSA-2018:3324] Low: RHEL 7 : fuse security update
[RHSA-2018:3052] Medium: RHEL 7 : wget security update
[RHSA-2018:3071] Low: RHEL 7 : krb5 security update
[RHSA-2018:3157] Medium: RHEL 7 : curl and nss-pem security update
[RHSA-2018:3253] Low: RHEL 7 : jasper security update
[RHSA-2018:3107] Low: RHEL 7 : wpa_supplicant security update
[RHSA-2018:0849] Low: RHEL 7 : gcc security update
[RHSA-2018:2557] Low: RHEL 7 : postgresql security update
[RHSA-2018:3665] Medium: RHEL 7 : NetworkManager security update
[RHSA-2018:3140] Medium: RHEL 7 : GNOME security update

[CVE-2018-8037] Important: Apache Tomcat: Information Disclosure
[CVE-2018-8034] Medium: Apache Tomcat - Security Constraint Bypass
[CVE-2018-1336] Medium: Apache Tomcat - Denial of Service
[CVE-2018-11784] Medium: Apache Tomcat - Open Redirect

**Oct 22nd, 2018 -** Supplement 7 of this PCN introduces Feature Service Pack 7.1.3.2 for Utility Services which is applicable to all Hypervisor types supported by Utility Services 7.1 – i.e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Service Pack 7.1.3.2 should be applied to all Utility Services 7.1 Virtual Machines.
**Service Pack 7.1.3.2 (util_patch_7.1.3.2.0.01.zip, PLDS ID US000000091)**

This Service Pack addresses the following issues
**NOTE: For information on L1TF mitigation for AVP refer to PSN020369u.**

- In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

- Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

- Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

- The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

Fix PHP Time zone (tzdata Linux RPM updated to **tzdata-2018e**)
Passwords stored in clear text in logfiles is now masked.
Update add_spirit_certs support for non-FIPS mode
Apache Tomcat Security constraint annotations applied too late (CVE-2018-1305)
[RHSA-2018:1453-01] Critical: dhcp security update
[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update
[RHSA-2018:2387] Important: L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646
[RHSA-2018:1062-01] Important: kernel security, bug fix, and enhancement update
[RHSA-2018:1318-01] Important: kernel security, bug fix, and enhancement update
[RHSA-2018:2571-01] Important: bind security update
[RHSA-2018:1629-01] Important: kernel security update
[RHSA-2018:1700-01] Important: procps-ng security update
[RHSA-2018:1649-01] Important: java-1.8.0-openjdk security update
[RHSA-2018:2285] Important: yum-utils security update
[RHSA-2018:2181-01] Important: gnupg2 security update
[RHSA-2018:2242-01] Moderate: java-1.8.0-openjdk security and bug fix update
[RHSA-2018:1852-01] Moderate: kernel security update
[RHSA-2018:2123-01] Moderate: python security update
[RHSA-2018:0805-01] Moderate: glibc security, bug fix, and enhancement update
[RHSA-2018:0855-01] Moderate: ntp security, bug fix, and enhancement update

[RHSA-2018:0666-01] Moderate: krb5 security, bug fix, and enhancement update
[RHSA-2018:0998-01] Moderate: openssl security and bug fix update
[RHSA-2018:0849-01] Low: gcc security, bug fix, and enhancement update
[RHSA-2018:0980-01] Low: openssh security, bug fix, and enhancement update
[RHSA-2018:0913-01] Low: policycoreutils security, bug fix, and enhancement update

**May 7th 2018** – Supplement 6 of this PCN introduces Feature Pack 7.1.3 for Utility Services which is applicable to all Hypervisor types supported by Utility Services 7.1 – i.e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Feature Pack 7.1.3 should be applied to all Utility Services 7.1 Virtual Machines.

**NOTE: For information on Spectre/Meltdown mitigation for Utility Services, refer to PSN020346u.**

- In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- The customer should be aware that implementing these patches may result in performance degradation.

**Feature Pack 7.1.3 (util_patch_7.1.3.0.0.05.zip, PLDS ID US000000087)**

This Feature Pack addresses the following issues:
Trust establishment failed on Utility services 7.1.0.0.0.12 on SDM client
The DHCP Service displays wrong status with audit account
Support for vSphere 6.7
Selective Enabling of Security Hardening Options
ZAP:High Path Traversal
ZAP:High SQL Injection
ZAP:High Cross Site Scripting (Reflected)
ZAP:Medium Directory Browsing
ZAP:Medium X-Frame-Options Header Not Set
ZAP:Medium Format String Error
CRITICAL: [RHSA-2017:2836-01] Critical: dnsmasq security update
Customer banner on Utility services shows invalid output when seen via SSH session
RHEL 7 : wpa_supplicant (RHSA-2017:2907) (KRACK)
RHEL 7 : emacs (RHSA-2017:2771)
RHEL 7 : bind (RHSA-2017:2533)
RHEL 7 : httpd (RHSA-2017:2882) (Optionsbleed)
RHEL 6 / 7 : nss (RHSA-2017:2832)
RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2017:2998)
Correct Root Certificate Display & Fix Windows Format Files
Allow Access Control script, Configure_SSH_ACL.sh, to run in "Services Port Only" mode
HIGH Priority: [RHSA-2017:3075-01] Important: wget security update

RHEL 7 : php (RHSA-2017:3221)
MEDIUM: [RHSA-2017:3263-01] Moderate: curl security update
HIGH: [RHSA-2017:3269-01] Important: procmail security update
HIGH Priority: [RHSA-2017:3270-01] Important: apr security update
MEDIUM: [RHSA-2017:3315-01] Important: kernel security and bug fix update
If AIDE is enabled, need to run AIDE update after applying updates and / or performing a restore
MEDIUM: [RHSA-2017:3379-01] Moderate: sssd security and bug fix update
MEDIUM: [RHSA-2017:3402-01] Moderate: postgresql security update
Update Initial_conf.sh to update the entries in /etc/hosts
HIGH: [RHSA-2018:0007-01] Important: kernel security update
HIGH: [RHSA-2018:0012-01] Important: microcode_ctl security update
HIGH: [RHSA-2018:0014-01] Important: linux-firmware security update
HIGH Priority: [RHSA-2018:0095-01] Important: java-1.8.0-openjdk security update
HIGH Priority: [RHSA-2018:0102-01] Important: bind security update
RHEL 7 : dhcp (RHSA-2018:0158)
RHEL 7 : kernel (RHSA-2018:0151) (Meltdown) (Spectre)
MEDIUM: [RHSA-2018:0260-01] Moderate: systemd security update
Addition of Kernel Configuration Script
[RHSA-2018:0483-01] Important: dhcp security update
Fix Test Alarms for All Users
[RHSA-2018:0395-01] Important: kernel security and bug fix update
[RHSA-2018:0406-01] Moderate: php security update
Improvements To Configure_SSH_ACL.sh Script
Restore of 7.1.3 backup can fail
Fix to swversion permissions issues

**March 7th 2018** – Supplement 5 of this PCN introduces updates to Utility Services 7.1 OVAs for VMware, Amazon Web Services (AWS), and Kernel-based Virtual Machine (KVM) infrastructures. The re-issue has been necessary to remove obsolete Gateway Firmware, all of which has now been removed from the OVA. Otherwise, the features are identical to the original releases.

**Utility Services 7.1 OVA for VMware ( ~~US-7.1.0.0.0.18-e55-2_OVF10.ova~~, PLDS ID US000000077, md5sum 8e4dc4360c10785fb81e7a5d7f7edb6a )** *(Updated, see supplement 11 above)***.**

**Utility Services 7.1 OVA for AWS (US-7.1.0.0.0.17-aws-37_OVF10.ova, PLDS ID US000000076, md5sum a2aed766077e4a572e011dff1cc7dc7f)**

**Utility Services 7.1 OVA for KVM (US-7.1.0.0.0.17-kvm-35.ova, PLDS ID US000000078, md5sum 3bc8d7b6f5efe4f7882d4932a998b79d )**

**December 11th 2017** – Supplement 4 of this PCN introduces Feature Pack 7.1.2 for Utility Services which is applicable to all Hypervisor types supported by Utility Services 7.1 – i.e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Feature Pack 7.1.2 should be applied to all Utility Services 7.1 Virtual Machines.
**Feature Pack 7.1.2 (util_patch_7.1.2.0.0.07.zip, PLDS ID US000000084)**
This Feature Pack addresses the following issues:
The DHCP Service displays wrong status with audit account
The mode of Utility Services is blank after upgrading US from 7.0 to 7.1 build 15
MEDIUM: [RHSA-2017:1208-01] Important: jasper security update

MEDIUM: [RHSA-2017:1262-01] Important: rpcbind security update
LOW: [RHSA-2017:1263-01] Important: libtirpc security update
MEDIUM: [RHSA-2017:1308-01] Important: kernel security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:1382-01] Important: sudo security update
LOW: Apache Tomcat Security Constraint Bypass (CVE-2017-5664)
MEDIUM: [RHSA-2017:1481-01] Important: glibc security update
MEDIUM: [RHSA-2017:1484-01] Important: kernel security update
HIGH Priority: [RHSA-2017:1365-03] Important: nss security and bug fix update
Update tmclient.jar for Spirit Agent
MEDIUM: [RHSA-2017:1574-01] Moderate: sudo security update
MEDIUM: [RHSA-2017:1615-01] Important: kernel security and bug fix update
Cannot unpack SIP 7.1 firmware by using SHA1 unpack on Utility Server
MEDIUM: [RHSA-2017:1680-01] Important: bind security and bug fix update
ZAP: Cookie No HttpOnly Flag
Cannot add the second remote syslog server
The error message is shown when running the command Add_RSYSLOG.sh on US with FIPS mode enabled
Addition Commercial FIPS Script
Create new ovf_set_multi_static script
MEDIUM: [RHSA-2017:1789-01] Critical: java-1.8.0-openjdk security update
MEDIUM: [RHSA-2017:1842-01] Important: kernel security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:1931-01] Moderate: bash security and bug fix update
MEDIUM: [RHSA-2017:1852-01] Moderate: openldap security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:2029-01] Moderate: openssh security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:1868-01] Moderate: python security and bug fix update
MEDIUM: [RHSA-2017:2192-01] Moderate: mariadb security and bug fix update
MEDIUM: [RHSA-2017:1916-01] Moderate: glibc security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:2016-01] Moderate: curl security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:1860-01] Moderate: libtasn1 security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:1865-01] Moderate: X.org X11 libraries security, bug fix and enhancement update
MEDIUM: [RHSA-2017:1871-01] Moderate: tcpdump security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:2292-01] Moderate: gnutls security, bug fix, and enhancement update
MEDIUM: [RHSA-2017:2299-01] Moderate: NetworkManager and libnl3 security,bug fix and enhancement update
LOW: [RHSA-2017:2285-01] Moderate: authconfig security, bug fix, and enhancement update
Add Missing SUDO entry for Local Pre-Populate Plug-In
Extend SSH Timeout
TFTP server cannot be started
LOW: [RHSA-2017:1983-01] Moderate: postgresql security and enhancement update
MEDIUM: [RHSA-2017:2459-01] Important: libsoup security update
LOW: Apache Tomcat Cache Poisoning (CVE-2017-7674)
LOW: [RHSA-2017:2473-01] Important: kernel security and bug fix update
MEDIUM: [RHSA-2017:1574-01] Moderate: sudo security update
MEDIUM: [RHSA-2017:2479-01] Important: httpd security update
Cannot access MyPhone admin page with admin login and password with special characters
Database Autostart Buttons and Status are not working
Addition of Hardening Mode configuration files to backup/restore
96x1 H323 Phone is failed to backup the local device settings to Utility Services
Serviceability Agent Configuration Updates for Hardened Mode

Addition of 3rd Party Certificate Support for Tomcat
Serviceability Agent configuration needs to be updated when FIPS Mode enabled
Allow Common OS setLoginBanner.sh script to be run with root privileges
Update the Serviceability Agent Configuration for AVP license alarms for Avaya Aura® Utility Services
Provide script to import 3rd party certificate and create keystores for Serviceability Agent
Allow admin users to generate security reports for AIDE and auditd.
Fix Apache Permissions after Update.
Issue while enabling FIPS mode in Utility Services 7.1.2.0.0.04
Need to Disable chronyd for NTPD to Auto Start
AVP licensing alarms not picked up by the Serviceability Agent
Fix Logrotate Rules for Remote.log
Add Sudo for Configure NMS Script
Utility services patching failed via SMGR SDM on US commercial setup
Issues / changes for the add_spirit_certs script

**August 14th 2017** – Supplement 3 of this PCN introduces V7.1 of Utility Services for Kernel-based Virtual Machine (KVM) and Feature Pack 7.1.1 which is applicable to all Hypervisor types supported by Utility Services 7.1 – i.e. VMware, Amazon Web Services (AWS), and Kernel Virtual Machines (KVM). Feature Pack 7.1.1 should be applied to all Utility Services 7.1 Virtual Machines and is required for KVM deployments.

**Utility Services 7.1 OVA (US-7.1.0.0.0.17-kvm-33.ova, PLDS ID US000000078 )**

This vAppliance is for deployment on Kernel-based Virtual Machine (KVM) infrastructures. It is part of the overall Virtualization enablement (VE) program bringing the Avaya Aura portfolio onto KVM. This vAppliance is built to the .OVA (Open Virtualization Appliance) standard including both the guest operating system and the application software for deployment thru KVM. It includes all files in the .OVA format necessary to install Utility Services 7.1 and includes predefinition of KVM resources required for the product to meet performance/capacities

**Feature Pack 7.1.1 (util_patch_7.1.1.0.0.01.zip, PLDS ID US000000079 )**

This Feature Pack addresses the following issues:
MEDIUM: [RHSA-2017:1262-01] Important: rpcbind security update
LOW: [RHSA-2017:1263-01] Important: libtirpc security update
MEDIUM: [RHSA-2017:1574-01] Moderate: sudo security update
MEDIUM: [RHSA-2017:1615-01] Important: kernel security and bug fix update

**July 6th 2017** – Supplement 2 of this PCN introduces a replacement Utility Services 7.1 for VMware OVA after finding issues with IP Address configuration when deployed directly on an ESXi Hypervisor. This new build is a replacement OVA that should be used for all VMware deployments. It is recommended that all customers upgrade to this latest version if they previously installed the earlier build to ensure compatibility with future service packs.

**Utility Services 7.1 OVA ( US-7.1.0.0.0.18-e55-379_OVF10.ova, PLDS ID US000000077 )**

Utility Services 7.1 vAppliance for deployment on Appliance Virtualization Platform (AVP) on Avaya provided servers or VMware® vSphere™ ESXi 5.5/6.0/6.5 infrastructures on VMware® certified hardware. This vAppliance is built to the OVA (Open Virtualization Appliance) standard including both the guest operating system and the application software for deployment through Solution Deployment Manager (SDM), vCenter or vSphere clients. It includes all files in the .OVA format necessary to install Utility Services 7.1 and includes predefinition of VMware resources required for the product to meet documented performance and capacities.

**Utility Services 7.1 OVA for AWS (US-7.1.0.0.0.17-aws-35_OVF10.ova, PLDS ID US000000076 )**

Utility Services 7.1 vAppliance is for deployment on Amazon Web Services (AWS) infrastructures. It is part of the overall Virtualization enablement (VE) program bringing the Avaya Aura portfolio onto AWS. This vAppliance is built to the .OVA (Open Virtualization Appliance) standard including both the guest operating system and the application software for deployment thru Amazon Web Services. It includes all files in the .OVA format necessary to install Utility Services 7.1 and includes predefinition of AWS resources required for the product to meet performance/capacities.

**Appliance Virtualization Platform (AVP) 7.1.0.0.0.9 (avaya-avp-7.1.0.0.0.9.iso or avaya-avp-7.1.0.0.0.9.zip).** The Utility Services software specified in this PCN was verified and is compatible with AVP release 7.1.0.0.0.9. See PCN 2064S for more information. AVP must be upgraded to the compatible release before upgrading Utility Services.

**June 7th 2017** – Supplement 1 of this PCN introduces a replacement Utility Services 7.1 for VMware OVA after finding issues with patching on the previous build when deployed in Services Port Only mode. The two patches for the original build 16 have also been incorporated into this release so this single OVA forms the complete 7.1 GA Release. This new build also contains additional security fixes so it is recommended that all customers upgrade to this latest version to if they previously installed the initial build. This will also ensure compatibility with future service packs.

**Utility Services 7.1 OVA ( US-7.1.0.0.0.17-e55-378_OVF10.ova, PLDS ID US000000075 )**
Utility Services 7.1 vAppliance for deployment on Appliance Virtualization Platform (AVP) on Avaya provided servers or VMware® vSphere™ ESXi 5.5/6.0/6.5 infrastructures on VMware® certified hardware. This vAppliance is built to the OVA (Open Virtualization Appliance) standard including both the guest operating system and the application software for deployment through Solution Deployment Manager (SDM), vCenter or vSphere clients. It includes all files in the .OVA format necessary to install Utility Services 7.1 and includes predefinition of VMware resources required for the product to meet documented performance and capacities.

**May 8th 2017** – The original PCN introduced Utility Services 7.1 for VMware.

**NOTE**: The OVA and the patches below are no longer available and the OVA listed in Supplement 1 should be used.

**Utility Services 7.1 OVA ( US-7.1.0.0.0.16-e55-373_OVF10.ova, PLDS ID US000000070 )**
Utility Services 7.1 vAppliance for deployment on Appliance Virtualization Platform (AVP) on Avaya provided servers or VMware® vSphere™ ESXi 5.5/6.0/6.5 infrastructures on VMware® certified hardware. This vAppliance is built to the OVA (Open Virtualization Appliance) standard including both the guest operating system and the application software for deployment through Solution Deployment Manager (SDM), vCenter or vSphere clients. It includes all files in the .OVA format necessary to install Utility Services 7.1 and includes predefinition of VMware resources required for the product to meet documented performance and capacities.

**NOTE: The following two patches are part of, and complete the 7.1 GA Release. Patch 7.1.0.0.2 is mandatory, whilst Patch 7.1.0.0.1 is only required on Upgrades to V7.1.**

**Utility Services Patch 7.1.0.0.1 ( util_patch_7.1.0.0.1.01.zip PLDS ID US000000072 )**
Utility Services Patch 7.1.0.0.1 provides a fix to allow the DHCP Daemon to start up correctly after an upgrade from V6.3/7.0.x. It is not necessary to apply this to a new install. This patch corrects an issue with the DHCPD Configuration file when it is installed - removing the patch has no effect.

**Utility Services Patch 7.1.0.0.2 ( util_patch_7.1.0.0.2.01.zip PLDS ID US000000073 )**
Utility Services Patch 7.1.0.0.2 provides a fix to allow the state of the Enhanced Access Security Gateway (EASG) to be preserved after a reboot with a partial environment file. This patch is recommended for all new installs and is immediate in effect - removing the patch has no effect.

**NOTE:** Utility Services 7.1 does include a default certificate. Avaya recommends using an Avaya Aura® System Manager generated certificate or third party generated certificate. Review the Release Notes, What's New in 7.1 and specific deployment documents on Avaya Support for additional information.

**NOTE:** Utility Services 7.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. EASG provides a secure method for Avaya services personnel to access the Avaya Aura® Application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck

**NOTE**: The VMware® vSphere™ Client can no longer connect to Avaya Aura® Appliance Virtualization Platform (AVP). Solution Deployment Manager (SDM) or the VMware embedded host client must be used.

.

| | |
|---|---|
| **Level of Risk/Severity Class 1=High Class 2=Medium Class 3=Low** | Class 2 |
| **Is it required that this PCN be applied to my system?** | This PCN is required for all Utility Services 7.1 Virtual Machines running on the Appliance Virtualization Platform (AVP), VMware® vSphere™ ESXi infrastructures, Amazon Web Services (AWS), or Kernel-based Virtual Machines (KVM). |
| **The risk if this PCN is not installed:** | This PCN contains a large number of important security fixes. It is strongly recommended that this Feature Pack is applied to any installation of V7.1 Utility Services. |
| **Is this PCN for US customers, non-US customers, or both?** | This PCN applies to both US and non-US customers. |
| **Does applying this PCN disrupt** | Activation of this Utility Services upgrade is service disrupting. |

| | |
|---|---|
| **my service during installation?** | |
| **Installation of this PCN is required by:** | Customer or Avaya Authorized Service Provider. This upgrade is customer installable and remotely installable.<br>Please note that any existing Service or Feature Packs should be **REMOVED** prior to installing Feature Pack 7.1.3. This Feature Pack is cumulative and includes all of the security remediation and bug fixes of previous Service or Feature Packs |
| **Release notes and workarounds are located:** | The Utility Services Release Notes contain the specific software updates and enhancements included in the release and can be obtained by performing the following steps from a browser:<br>1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**<br>2. Mouse over **Support by Product** at the top of the page, select **Documents** in the menu.<br>3. Begin to type **Utility Services** in the **Enter Your Product Here** box and when Avaya Aura® Utility Services appears as a selection below, select it.<br>4. Select 7.1.x from the **Choose Release** pull down menu to the right.<br>5. Scroll down (if necessary) and check the box for **Release & Software Update Notes**.<br>6. Select **ENTER**. Available documents are displayed.<br>7. Select the document titled **Avaya Aura® 7.1.3 Release Notes**. A link to the Release Notes can also be found on the **Avaya Aura® Utility Services 7.1 Service Packs, 7.1.x** download page (see section **How do I order this PCN** in this PCN). |
| **What materials are required to implement this PCN (If PCN can be customer installed):** | This PCN is being issued as a customer installable PCN. The specified Utility Services files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.<br><br>If unfamiliar with installing Utility Services software updates, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN. |
| **How do I order this PCN (If PCN can be customer installed):** | The software updates can be downloaded by performing the following steps from a browser:<br>1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**<br>2. Mouse over **Support by Product** at the top of the page, select **Downloads** in the menu.<br>3. Begin to type **Utility Services** in the **Enter Product Name** box and when Avaya Aura® Utility Services appears as a selection below, select it.<br>4. Select 7.1.x from the **Choose Release** pull down menu to the right.<br>5. Scroll down if necessary and select **Avaya Aura® Utility Services 7.1 Software, 7.1.x.**<br>6. Scroll down the page to find the download link for the appropriate OVA. This link will take you to the PLDS system with the **Download pub ID** already entered.<br>7. This page also includes a link to this PCN and the Release Notes.<br>Software updates can also be downloaded directly from the PLDS system at http://plds.avaya.com. |

1. Enter your login ID and password. You may have to search for and enter your company name and/or accept the one time EULA to gain access to software downloads.
2. Select **View Downloads.**
3. In the **Search by Download** tab enter the correct PLDS ID (corresponding PLDS IDs included in the Description section of this document) in the **Download pub ID** search field to access the download. Select the **Download** link to begin the download.

**PLDS Hints:**

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Utility Services** in the **Product Line** search field to display frequently downloaded Utility Services software, including recent Service Packs and updates.
2. Previous Utility Services 7.1 Service Packs are also available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Utility Services** in the **Application** search field and **7.1** in the **Version** search field to display all available Utility Services 7.1 software downloads

The MD5 sums are included in the Avaya Support and PLDS descriptions for the download files.

**NOTE:** If deploying Utility Services on AVP the compatible AVP software is also required.

**Finding the installation instructions (If PCN can be customer installed):**

The instructions for installing or upgrading Utility Services software on Appliance Virtualization Platform (AVP) and VMware® Virtualized Environments (VE) can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**
2. Mouse over **Support by Product** at the top of the page, select **Documents** in the menu.
3. Begin to type **Utility Services** in the **Enter Your Product Here** box and when Avaya Aura® Utility Services appears as a selection below, select it.
4. Select **7.1.x** from the **Choose Release** pull down menu to the right.
5. Check the box for **Installation, Upgrades & Config**.
6. Select **ENTER**. Available documents are displayed.
7. Select the appropriate document (e.g., select **Deploying Avaya Aura® Utility Services** for new installations or **Upgrading Avaya Aura® Utility Services** for upgrades).

## SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

**Note: Customers are required to backup their systems before applying the Service Pack.**

**How to verify the installation of the Service Pack has been successful:**

For AVP and VMware® Virtualized Environments you can verify that a Service Pack/Feature Pack is activated using the Utility Services System Management Interface (SMI) from the **Administration** > **Common** > **Software Version** page, or via Avaya Aura® Solution Deployment Manager (SDM).

**What you**

Escalate to Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner.

| | |
|---|---|
| **should do if the Service Pack installation fails?** | |
| **How to remove the Service Pack if malfunction of your system occurs:** | For AVP and VMware® Virtualized Environments deactivate the Service Pack/Feature Pack using the Command-Line tools documented in the Administration Guide. |

**SECTION 1B – SECURITY INFORMATION**

| | |
|---|---|
| **Are there any security risks involved?** | No |
| **Avaya Security Vulnerability Classification:** | N/A |
| **Mitigation:** | N/A |

**SECTION 1C – ENTITLEMENTS AND CONTACTS**

| | |
|---|---|
| **Material Coverage Entitlements:** | Utility Services 7.1 OVAs and Service Packs/Feature Packs are available free of charge to customers with a valid support contract for Utility Services 7.x<br><br>. |
| **Avaya Customer Service Coverage Entitlements:** | Avaya is issuing this PCN as installable by the customer. If the customer requests Avaya to install this PCN, it is con billable event as outlined in Section 4 (*Software Updates and Product Correction Notices*) of the Avaya Service Ag Supplement (Full Maintenance Coverage) unless the customer has purchased an Avaya Services enhanced offer su Avaya Services Product Correction Support offer.<br><br>Additionally, Avaya on-site support is not included. If on-site support is requested, Avaya will bill the customer cu Incident charges unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Service Correction Support offer. |

| **Customers under the following Avaya coverage:**<br>-Full Coverage Service Contract*<br>-On-site Hardware Maintenance Contract* | |
|---|---|
| **Remote Installation** | Current Per Incident Rates Apply |
| **Remote or On-site Services Labor** | Current Per Incident Rates Apply |

- Service contracts that include both labor and parts support – 24x7, 8x5.

| | |
|---|---|
| **Customers under the following Avaya coverage:**<br>-Warranty<br>-Software Support<br>-Software Support Plus Upgrades<br>-Remote Only<br>-Parts Plus Remote<br>-Remote Hardware Support<br>-Remote Hardware Support w/ Advance Parts Replacement | |
| **Help-Line Assistance** | Per Terms of Services Contract or coverage |
| **Remote or On-site Services Labor** | Per Terms of Services Contract or coverage |

**Avaya Product Correction Notice Support Offer**

The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all Avaya issued PCNs that are classified as "Customer-Installable". Refer to the PCN Offer or contact your Avaya Account Representative for complete details.

**Avaya Authorized Partner Service Coverage Entitlements:**

**Avaya Authorized Partner**

Avaya Authorized Partners are responsible for the implementation of this PCN on behalf of their customers.

**Who to contact for more information:**

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.