Pulse Secure

Pulse Access Control

Release Notes

Unified Access Control 4.4R13.1

OAC Version	**5.60.26749**
Build	**26749**
Published	**July 2015**

This is an incremental release notes describing the changes made from C4.4R1 release to C4.4R13.1. The C4.4R1 GA release notes still apply except for the changes mentioned in this document. Please refer to C4.4R1 GA release notes for the complete version.

Contents

Noteworthy Changes:

1. The IKE Phase 1 soft rekeying doesn't work properly, and it causes packets dropping while rekeying. It results most TCP applications disconnected.
   The IKE Phase 1 soft rekeying is temporary disabled. After Phase1 lifetime is reached, a new phase1 can be triggered by a tunnel traffic packet or by a Persistent Tunnel trigger. The gap is small, and most TCP application connections will stay.
   The IKE Phase 1 soft rekeying is fixed in a later version.

2. Support for the following platforms and browsers are added in C4.4R7:

   Windows 8.1

   b. Internet Explorer-11 on Windows 8.1 and Windows 7

   c. Mac OS – 10.9

NSM Schema for C4.4R13.1

The NSM schema for this software version will not be published.

Known Issues/Limitations Fixed in C4.4R13.1 Release

This release addresses the issue described in the following Pulse Security Advisory:

www.pulsesecure.net/kb/JSA10648

Known Issues/Limitations Fixed in C4.4R13 Release

1. ifmap-client - Federated clients show multiple IP addresses on Fed server. (946184)
2. pulse-802-1x - Realm is not set correctly based on the authentication protocol configuration. (1004553)
3. uac-oac-client-other - OAC may disconnect WiFi incorrectly when signal strength is poor. (1004198)

Known Issues/Limitations Fixed in C4.4R12 Release

1. System-admin - Console login may fail for admin users with console access enabled. (999726)

Known Issues/Limitations Fixed in C4.4R11.1 Release

1. This release fixes the issue described in **JSA10629**. For more detailed info please refer **KB29195**. (999726)

Known Issues/Limitations Fixed in C4.4R10 Release

1. uac-cdl - Push config feature is failing when trying to do selective push of Resource access policies. (943637)

Known Issues/Limitations in C4.4R8.1 Release

1. asg-endpointintegrity-opswat - Host Checker Opswat policy will fail for the customers running with ESAP 2.5.0 and below and hence they need to upgrade to ESAP 2.5.1 and above. (952926)

Known Issues/Limitations Fixed in C4.4R8.1 Release

1. asg-system-security - This release fixes the issue described in JSA10623. For more detailed info please refer KB29004. (981148)

Known Issues/Limitations Fixed in C4.4R8 Release

1. ifmap-client - IVE's IF-MAP client subscribes for sessions even after un-exporting them, leading to much CPU use. (919734)
2. ifmap-client – fedclient process may crash while doing VIP failover on Fed Server Cluster. (926727)
3. pulse-connmgr - Pulse client can fail to logon to the server from an IP address that was previously used by a different client due to a bug in the clean up of the old session. (921871)
4. system-webserver - "Internal Server Error" displayed when using SPNEGO SSO when user is mapped to too many AD groups. (894044)
5. uac-agentman - A possible memory leak in dsagentd causing high memory and swap usage. (925368)
6. uac-agentman - Cache fragmentation causing stability issues and high cache size. (928394)
7. uac-dsagentd - dsagentd assertion on IC when Return RADIUS attribute VLAN is changed if COA is enabled. (921176)
8. uac-gateman - Gateman cores when multi-homing or session roaming is enabled. (911760)
9. uac-gateman - Gateman can crash if enforcer is disconnected while refreshing enforcer policies (914683)

10. uac-sbr - Log messages like "Warning: Duplicate Request in Cache with mismatched message authenticator, rejecting." observed in SBR logs. (921463)
11. uac-sbr - Process snapshot for radius got generated on IC while performing trusted domain machine authentication.(921784)
12. uac-sbr – Pulse connection fails when IC has a realm restriction "Allow Users and remember certificate" using PAP authentication method (923625)
13. uac-sbr -The radius process permits initiation of too many concurrent EAP authentications. This resulted in the radius process using too much memory. (923696)
14. uac-sbr - 'Session Deletion Disconnect Message' is not logged, when user with OAC session is deleted from Active User Page. (933208)
15. juns-other - OAC failed to populate the correct encryption details during a network scan for a new network when the wireless access point is configured for WPA2/TKIP or WPA/AES Encryption. (935842)
16. uac-admin - Active Users page shows Agent type as Windows 8 Odyssey Access Client when connected from Win 8.1 machine. (936811)
17. uac-oac-client-other - Odyssey installation fails with error:1334 on Windows 7. (947318)

Known Issues/Limitations Fixed in C4.4R6 Release

1. sysmgmt-snmp - SNMP traps related to archiving credentials or user permissions are mislabeled. (914051)
2. system-digital-cert - When generating a new CSR of type ECC with either p-256 or p-384 curves, after clicking on create, the next screen under CSR incorrectly shows key size as 1024 bits. The CSR is a valid one with the appropriate curves
3. system-digital-cert - No UI information was present when doing CSR creation on FIPS units; this can take 10+ minutes. (930282)
4. system-other - dsagentd process may fail due to invalid reference. (913064)
5. system-other - Search for user-ids in the active users tab in the admin UI is case-sensitive. (921186)
6. system-webserver - dsnetd may fail during a MAG upgrade if the external and/or management ports are disabled. (859959)
7. cachecleaner-end-user - Cache Cleaner may delete required system files when executed via Pulse if empty registry values are encountered. (910987)
8. pulse-ic-am - Pulse may continually retry to authenticate after session expiration. (928749)
9. pulse-other - Large sign-in notifications may prevent Pulse VPN tunnel setup. (868563)
10. pulse-sa-nc-am - XP client machines may fail to successfully query the Pulse DNS servers. (881890)

Known Issues/Limitations Fixed in C4.4R5 Release

1. aaa-other - When a SQL server is used for authentication/authorization, a blank page pops up when the attribute button is pressed. (882675)
2. pulse-other - RADIUS challenge message is not getting displayed in Pulse UI, when RADIUS is used for secondary authentication. (895219)
3. uac-auth – Infranet Controller doesn't allow users to specify UPN as the username. This leads to user authentication failures. (740245)
4. uac-oac-client-other – Installing OAC on a Windows 8 32 bit client causes unsigned driver warning pop-up. (891095)
5. asg-ifmap-client - Pulse Secure Access Federation Client sends session data without IP address to Federation Server in case of Cluster failover, or restart services or by changing roles association for export policy. (855219)

Known Issues/Limitations Fixed in C4.4R4 Release

1. aaa-local - Start Time for a system local user doesn't get exported when an XML export of the IC configuration is done. (870404)
2. ifmap-client - Infranet Controller allows roles to be deleted, even if they are used in session import/export policies. (884343)
3. uac-auth - Mac authenticated users are counted against the license preventing the user session login. (883552)
4. uac-gateman - Gateman cores intermittently while communicating with two Netscreen firewalls configured in NSRP A/A mode. (880527)
5. uac-sbr - Radius request attributes does not show realm attached to it on Admin UI. (853429)
6. uac-sbr - Occasionally authentication is slow on IC and SA. (861011)
7. uac-sbr - Radius sometimes crashes in association with concurrent TLS authentications. (896214)
8. uac-other - IC sends CoA/Disconnect message when it receives accounting stop message causing Machine to User login failure. (852392)

Known Issues/Limitations Fixed in C4.4R3 Release

1. ifmap-server - Fed server crashes when MAG profiler as a Fed client tries to connect. (867088)
2. pulse-other - Certificate trust popup appears when Pulse L3 connection fails over to another node in a cluster. (860555)

3. system-dspar - RADIUS requests dropped during heavy RADIUS utilization and reported in the events log. (661192)
4. uac-admin - Realms with the apostrophe character cannot be assigned to a sign-in policy. (858472)
5. uac-auth - IC does not sends MAC address which it receives as ":callingStationID" attribute during authentication to SQL server for authorization. (877594)
6. uac-other - Post-Auth Sign-In Notification causes Native Windows supplicant to fail authentication. (852780)
7. uac-other - HTTP to HTTPS redirect does not happen during captive portal for IC landing page. (859287)

Known Issues/Limitations Fixed in C4.4R2 Release

1. pulse-ive-cm – When the option, "Between endpoints and the Pulse Access Control Service" is not selected, in some instances the IC doesn't send the list of ICs in the cluster for Pulse to failover. (851615)
2. pulse-connmgr - With DNS load balancer configured, Pulse will not get a new IP list from DNS by clicking on retry button when connection to an invalid IC fails. (840939)
3. pulse-tunnelmgr-ike - The IKE Phase 1 soft rekeying doesn't work properly and packets are dropped while rekeying which can result in TCP applications getting disconnected. In this release, the IKE Phase 1 soft rekeying is temporary disabled. After Phase1 lifetime is reached, a new phase1 can be triggered by a tunnel traffic packet or by a persistent tunnel trigger. The gap is small and most TCP applications will stay connected. The IKE Phase 1 soft rekeying is fixed in a later version. (853698)
4. sa-sbr - When a user logs onto the SA that has a certificate restriction or certificate authentication configured then a process on the SA can go into an infinite loop if the following conditions are met:

   a. The realm you are signing into has a certificate restriction or is configured for certificate authentication.

   b. The client you are using is OAC or Pulse 3.0 or earlier.

   c. There is no certificate on the endpoint that the client can select. (867048)
5. uac-admin - The maximum session length for a user role cannot be modified when Radius Server only license is installed on the IC. (845597)
6. uac-other – On the serial console, when entering a string for <path>, after generating a system snapshot, the system used the input as a filename instead of a directory location. (810209)
7. uac-other - SSO does not show up under Realm->Authentication Policy for a realm with AD authentication enabled when MAGX600-UAC-SRX license is installed. (858894)
8. uac-xmlexportimport - XML import of the config fails if an Enforcer on an IC with the serial number is configured in the second line by keeping the first line empty. (842698)