One Identity Safeguard for Privileged Sessions 5.0.7

Hotfix Release Notes

August 2018

This hotfix includes the changes listed in the following sections. One Identity may generate additional hotfixes for future releases of the product.

About this hotfix

This hotfix addresses various bug fixes, see Resolved issues on page 1. The minimum version required for installing this hotfix is 5 LTS.

Resolved issues

The following is a list of issues resolved in this hotfix.

Table 1: Resolved issues

Resolved issue	Issue ID
Unnecessary NFS archive share remounts can cause problems with the archiving process Safeguard for Privileged Sessions checks the status of the archive targets and remounts the share as required. In case of NFS shares, this process did not work properly and the share was remounted every time the check was performed even if the connection was working properly. This could cause problems with the	PAM-6347

Resolved issue	Issue ID
archiving process. The problem did not affect SMB shares and has been fixed for NFS shares in this release.	
Upgrading from 4.4.x to the latest 5 LTS release is not allowed It was not possible to upgrade from any release in the 4.4.x branch to the latest 5.0.x release. It is now fixed and this upgrade path is possible.	PAM-6288
Upgrading the content index result database could fail and break the entire upgrade process In some cases, upgrading the database that contains the results of the indexed screen contents for very old sessions (called Sphinx) could fail and this failure could cause the entire upgrade process to fail and in some cases even the rollback to the previous version failed, too. We made the upgrade process more robust and the failure of upgrading this one component will not break the entire upgrade process.	PAM-6273
POST requests on the REST API are vulnerable against session fixation attacks The authentication endpoint accepts and reuses previously issued session ID cookies even if the authenticated session is expired, which can allow attackers to execute a session fixation attack if they can trick the requestor to execute specially crafted POST requests. This behavior was not present on GET requests. This issue has been fixed and session IDs are no longer reused after a new authentication.	PAM-6056
Password change notification in SPNEGO-enabled RDP connections In case a domain user's password is expired, the RDP server can "report" this by sending a TLS alert during the CredSSP setup. This was supported for plain NTLM authentications but not when SPNEGO was used. This is now fixed and password change notifications work properly when SPNEGO is in use.	PAM-6054
Large number of error messages in the logs for HTTP traffic For monitored HTTP sessions, a large number of error messages similar to "AttributeError: 'NoneType' object has no attribute 'startswith'" appeared in the logs even if connection passed through properly. This has been fixed and no such error messages appear in the logs anymore.	PAM-5802
SSH proxy crash if LDAP server is slow to respond Long response times of external LDAP servers that are accessed via STARTTLS could cause the SSH proxy to crash and consequently the termination of all ongoing SSH connections. This has been fixed and LDAP timeouts are now handled properly.	PAM-5610
Invalid "Error storing XML database" alerts sent In different circumstances, while using the configuration interface, SPS sent out	PAM-5266

Resolved issue	Issue ID
alerts notifying the administrator about an error "Error storing XML database". It was the result of an internal race condition and was not the signal of any actual problem. This has been corrected and no such messages are sent out anymore.	
Uploading TLS keys for syslog connections make the core firmware tainted Uploading TLS keys for syslog-ng into the syslog-ng/etc/ca.d directory made the core firmware tainted. The syslog-ng/etc/ca.d directory has been added to the tainted whitelist.	PAM-4543
When the web login IP address was changed on the UI, the user got locked out If the IP address of the web configuration interface is changed, the user needs to log in again on the new address. However, the configuration lock was not released before that, which meant that the user was temporarily prevented from accessing the configuration interface. This has been fixed and the configuration lock is now released automatically in this scenario.	PAM-2698
Large number of 'buffer too small to read octet string' error messages sent In different scenarios, SPS started sending out a large number of error alerts with the message 'buffer too small to read octet string'. This was not the signal of any actual problem with SPS rather only the result of a problem in the underlying net-snmp library used for self-monitoring. This has been fixed and no such alerts are sent out anymore.	PAM-1695
Invalid UTF-8 data received by a credential store plugin not handled properly If a credential store plugin was configured and one of the user-provided inputs (session cookie, username or the target host) contained an invalid UTF-8 character, it resulted in a hard-to-understand traceback in the logs and the termination of the session. Such problems are now detected in time, logged properly, and handled as normal authentication failures instead of an unexpected programming error in the plugin.	PAM-421

Installing this hotfix

To install the hotfix, see instructions in section "Upgrading SPS" in the One Identity Safeguard for Privileged Sessions Administration Guide.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.