CyberArk Security Bulletin CA23-14

Exposure of sensitive information to an unauthorized actor

Jul 5, 2023 · Knowledge Article

Article Number
000031740

Title
CyberArk Security Bulletin CA23-14

Details
CA23-14

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: High

Score [CVSS]: N/A

Third Party Publication / CVE: N/A

Impact: Exposure of sensitive information to an unauthorized actor

Affected products and versions:

Product*	Version(s)**	Additional Information
Password Vault Web Access (PVWA), Self-hosted	All versions prior to 13.2	

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions in our online documentation.

If a patch is not available for your installed version, or if you wish to move to the latest available version, upgrade your component according to the Upgrade version compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm?tocpath=Installation%7CUpgrade%7CIntroduction%7C_____1#Upgradeversioncompatibility).

Installed version	Patch Version	Download link	Documentation
PVWA 13.2	No action required		
PVWA 13.0 (STS) and its patches prior to 13.0.3, or older versions	13.0.3	https://www.cyberark.com/ca23-14-PVWA-13.0.3 (https://www.cyberark.com/ca23-14-PVWA-13.0.3)	Upgrade PVWA for 13.0 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 12.6 (LTS) and its patches prior to 12.6.7, or older versions	12.6.7	https://www.cyberark.com/ca23-14-PVWA-12.6.7 (https://www.cyberark.com/ca23-14-PVWA-12.6.7)	Upgrade PVWA for 12.6 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 12.2 (LTS) and its patches prior to 12.2.12, or older versions	12.2.12	https://www.cyberark.com/ca23-14-PVWA-12.2.12 (https://www.cyberark.com/ca23-14-PVWA-12.2.12)	Upgrade PVWA for 12.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 11.5 (LTS) and its patches prior to 11.5.17, or older versions	11.5.17	https://www.cyberark.com/ca23-14-PVWA-11.5.17 (https://www.cyberark.com/ca23-14-PVWA-11.5.17)	Upgrade PVWA for 11.5 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-Password-Vault-Web-Access.htm)

CyberArk Security Bulletin CA23-15

Improper neutralization of special elements used in an LDAP query ('LDAP Injection')

Jul 5, 2023 · Knowledge Article

Article Number
000031741

Title
CyberArk Security Bulletin CA23-15

Details
CA23-15

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: Critical

Score [CVSS]: 9.9

Third Party Publication / CVE: N/A

Impact: Improper neutralization of special elements used in an LDAP query ('LDAP Injection')

Affected products and versions:

Product*	Version(s)**	Additional Information
Password Vault Web Access (PVWA), Self-hosted	All versions prior to and including 13.2	

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions in our online documentation.

If a patch is not available for your installed version, or if you wish to move to the latest available version, upgrade your component according to the Upgrade version compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm?tocpath=Installation%7CUpgrade%7CIntroduction%7C____1#Upgradeversioncompatibility).

Installed version	Patch Version	Download link	Documentation
PVWA 13.2 (STS) and its patches prior to 13.2.2, or older versions	13.2.2	https://www.cyberark.com/ca23-15-PVWA-13.2.2 (https://www.cyberark.com/ca23-15-PVWA-13.2.2)	Upgrade PVWA for 13.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.2/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 13.0 (STS) and its patches prior to 13.0.3, or older versions	13.0.3	https://www.cyberark.com/ca23-15-PVWA-13.0.3 (https://www.cyberark.com/ca23-15-PVWA-13.0.3)	Upgrade PVWA for 13.0 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 12.6 (LTS) and its patches prior to 12.6.7, or older versions	12.6.7	https://www.cyberark.com/ca23-15-PVWA-12.6.7 (https://www.cyberark.com/ca23-15-PVWA-12.6.7)	Upgrade PVWA for 12.6 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 12.2 (LTS) and its patches prior to 12.2.12, or older versions	12.2.12	https://www.cyberark.com/ca23-15-PVWA-12.2.12 (https://www.cyberark.com/ca23-15-PVWA-12.2.12)	Upgrade PVWA for 12.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/PVWA-upgrade-overview.htm?tocpath=Installation%7CUpgrade%7CUpgrade%20PVWA%7C_____1)
PVWA 11.5 (LTS) and its patches prior to 11.5.17, or older versions	11.5.17	https://www.cyberark.com/ca23-15-PVWA-11.5.17 (https://www.cyberark.com/ca23-15-PVWA-11.5.17)	Upgrade PVWA for 11.5 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-Password-Vault-Web-Access.htm)

CyberArk Security Bulletin CA23-16

If a patch is not available for your installed version, or if you wish to move to the latest available version, upgrade your component according to the Possible version compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm?tocpath=Installation%7CUpgrade%7CIntroduction%7C____1#Upgradeversioncompatibility).

Jul 5, 2023 · Knowledge Article

Article Number

000031742

Title

CyberArk Security Bulletin CA23-16

Details

CA23-16

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: High (OWASP Risk Rating Methodology)

Score: High (OWASP Risk Rating Methodology)

Third Party Publication / CVE: N/A

Impact: Possible credential exposure to an unauthorized user

Affected products and versions:

Product*	Version(s)**	Additional Information
Privileged Session Manager (PSM), Self hosted	All versions prior to and including 13.2	PSM Version 13.2 is affected only if 64-bit connection components are in use. See the FAQ (https://cyberark-customers.force.com/s/article/CyberArk-Security-Bulletin-FAQ-CA23-16) for more information

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm) in our online documentation.

If a patch is not available for your installed version, or if you wish to move to the latest available version, upgrade your component according to the Upgrade version compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm?tocpath=Installation%7CUpgrade%7CIntroduction%7C____1#Upgradeversioncompatibility).

Installed version	Patch Version	Download link	Documentation
13.2	13.2.2	https://www.cyberark.com/ca23-16-PSM-13.2.2 (https://www.cyberark.com/ca23-16-PSM-13.2.2)	13.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-PSM.htm?tocpath=Installation%7CUpgrade%7CPrivileged%20Session%20Manager%7C_____1)
12.6	12.6.7	https://www.cyberark.com/ca23-16-PSM-12.6.7 (https://www.cyberark.com/ca23-16-PSM-12.6.7)	12.6 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
12.2	12.2.12	https://www.cyberark.com/ca23-16-PSM-12.2.12 (https://www.cyberark.com/ca23-16-PSM-12.2.12)	12.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
11.5	11.5.17	https://www.cyberark.com/ca23-16-PSM-11.5.17 (https://www.cyberark.com/ca23-16-PSM-11.5.17)	11.5 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-PSM.htm)

CyberArk Security Bulletin CA23-17

Possible credential exposure to an unauthorized user

Jul 5, 2023 · Knowledge Article

Article Number
000031743

Title
CyberArk Security Bulletin CA23-17

Details
CA23-17

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: High (OWASP Risk Rating Methodology)

Score: High (OWASP Risk Rating Methodology)

Third Party Publication / CVE: N/A

Impact: Possible credential exposure to an unauthorized user

Affected products and versions:

Product*	**Version(s)****	**Additional Information**
Privileged Session Manager (PSM) as part of the Privilege Cloud Connector	All Privilege Cloud Connector versions prior to version 13.2.	

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

Upgrade the Privilege Cloud Connector to v13.2:

1. Download Privilege Cloud Connector version 13.2 from the CyberArk Marketplace (https://www.cyberark.com/ca23-17-PSM-13.2). Mark the following files for download:

   Privileged Session Manager-Rls-13.2.zip

   Central Policy Manager-Rl13.2.zip

   Privilege Cloud Connector Unified Hardening GPO-v2.1.2.zip

   Privilege Cloud Connector Unified Hardening GPO-v2.1.2.txt

2. Install the package according to the upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/PrivCloud-upgrade-connector.htm) in our online documentation.

CyberArk Security Bulletin CA23-18

A potential buffer overflow vulnerability in Microsoft SQL Server

Jul 5, 2023 · Knowledge Article

Article Number
000031744

Title
CyberArk Security Bulletin CA23-18

Details
CA23-18

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: High

Score: 7.8 (High)

Third Party Publication / CVE: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8273 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8273)

Impact: A potential buffer overflow vulnerability in Microsoft SQL Server

Affected products and versions:

Product*	Version(s)**	Additional Information
Privileged Session Manager (PSM)	All versions prior to and including version 13.2	Only for installation on Windows 2016 operating system that are not configured with SQL Express 2016 service pack SP3

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

1. Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm) in our online documentation.

If a patch is not available for your installed version, or if you wish to move to the latest available version, upgrade your component according to the Upgrade version compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm?tocpath=Installation%7CUpgrade%7CIntroduction%7C_____1#Upgradeversioncompatibility).

Installed version	Patch Version	Download link	Documentation
13.2	13.2.2	https://www.cyberark.com/ca23-18-PSM-13.2.2 (https://www.cyberark.com/ca23-18-PSM-13.2.2)	13.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-PSM.htm?tocpath=Installation%7CUpgrade%7CPrivileged%20Session%20Manager%7C_____1)
12.6	12.6.7	https://www.cyberark.com/ca23-18-PSM-12.6.7 (https://www.cyberark.com/ca23-18-PSM-12.6.7)	12.6 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
12.2	12.2.12	https://www.cyberark.com/ca23-18-PSM-12.2.12 (https://www.cyberark.com/ca23-18-PSM-12.2.12)	12.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
11.5	11.5.17	https://www.cyberark.com/ca23-18-PSM-11.5.17 (https://www.cyberark.com/ca23-18-PSM-11.5.17)	11.5 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-PSM.htm)

2. Download and install KB5021129 on SQL Server 2016 SP3 from the following location: https://www.microsoft.com/en-us/download/details.aspx?id=105011 (https://www.microsoft.com/en-us/download/details.aspx?id=105011)

CyberArk Security Bulletin CA23-19

A potential buffer overflow vulnerability in Microsoft SQL Server

Jul 5, 2023 · Knowledge Article

Article Number
000031745

Title
CyberArk Security Bulletin CA23-19

Details
CA23-19

Issued: July 5, 2023

Updated: N/A

Version: 1.0

Severity: High (CVSS - 7.8)

Score: High (CVSS - 7.8)

Third Party Publication / CVE: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8273 (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8273)

Impact: A potential buffer overflow vulnerability in Microsoft SQL Server

Affected products and versions:

Product*	Version(s)**	Additional Information
Privileged Session Manager (PSM) as part of the Privilege Cloud Connector	All Privileged Session Manager (PSM) versions prior to version 13.2	Only for installation on Windows 2016 operating system that are not configured with SQL Express 2016 service pack SP3

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.

** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

Resolution:

Upgrade the Privilege Cloud Connector to v13.2 (if needed, SQL Express 2016 service pack will be upgraded to SP3):

1. Download Privilege Cloud Connector version 13.2 from the CyberArk Marketplace (https://www.cyberark.com/ca23-19-PSM-13.2). Mark the following files for download:

   Privileged Session Manager-Rls-13.2.zip

   Central Policy Manager-Rl13.2.zip

   Privilege Cloud Connector Unified Hardening GPO-v2.1.2.zip

   Privilege Cloud Connector Unified Hardening GPO-v2.1.2.txt

2. Install the package according to the upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/PrivCloud-upgrade-connector.htm) in our online documentation. Make sure that during the upgrade, on the Hardening page of the wizard, the TLS hardening checkbox is checked.

3. Download and install KB5021129 on SQL Server 2016 SP3 from the following location: https://www.microsoft.com/en-us/download/details.aspx?id=105011 (https://www.microsoft.com/en-us/download/details.aspx?id=105011)