Cyberark Security Bulletin CA23-11

Impact: Possible credential exposure to an unauthorized user

Jun 21, 2023 · Knowledge Article

Article Total View Count
1,876

Article Number
000031510

Title
Cyberark Security Bulletin CA23-11

Details
CA23-11

Issued: June 20, 2023

Updated: N/A

Version: 1.0

Severity: High (OWASP Risk Rating Methodology)

Score: High (OWASP Risk Rating Methodology)

Third Party Publication / CVE: NA

Impact: Possible credential exposure to an unauthorized user

Affected products and versions:

Product	Version(s)	Additional Information
Privileged Session Manager for SSH, PAM self-hosted	All versions prior to 13.2	

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

Fix Instructions:

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.

Installed version	Patch	Download	Documentation
13.0 and its patches prior to 13.0.2 or older versions	13.0.2	https://www.cyberark.com/CA23-11-13.0.2 (https://www.cyberark.com/CA23-11-13.0.2)	Upgrade PSM for SSH 13.0 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)
13.0 and its patches prior to 13.0.2 or older versions using Red Hat version 8	13.0.2	https://www.cyberark.com/CA23-11-13.0.2-RHEL8 (https://www.cyberark.com/CA23-11-13.0.2-RHEL8)	Upgrade PSM for SSH 13.0 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)
12.6 (LTS) and its patches prior to 12.6.6 or older versions	12.6.6	https://www.cyberark.com/CA23-11-12.6.6 (https://www.cyberark.com/CA23-11-12.6.6)	Upgrade PSM for SSH 12.6 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)
12.6 (LTS) and its patches prior to 12.6.6 or older versions using Red Hat version 8	12.6.6	https://www.cyberark.com/CA23-11-12.6.6-RHEL8 (https://www.cyberark.com/CA23-11-12.6.6-RHEL8)	Upgrade PSM for SSH 12.6 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)
12.2 (LTS) and its patches prior to 12.2.11or older versions	12.2.11	https://www.cyberark.com/CA23-11-12.2.11 (https://www.cyberark.com/CA23-11-12.2.11)	Upgrade PSM for SSH 12.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)
12.2 (LTS) and its patches prior to 12.2.11or older versions using Red Hat version 8	12.2.11	https://www.cyberark.com/CA23-11-12.2.11-RHEL8 (https://www.cyberark.com/CA23-11-12.2.11-RHEL8)	Upgrade PSM for SSH 12.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)

11.5 (LTS) and its patches prior to 11.5.16 or older versions	11.5.16	https://www.cyberark.com/CA23-11-11.5.16 (https://www.cyberark.com/CA23-11-11.5.16)	Upgrade PSM for SSH 11.5 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm)

Temporary mitigation:

There is no temporary mitigation for this bulletin.

For more technical information, see the Technical FAQ (https://cyberark-customers.force.com/s/article/CyberArk-Security-Bulletin-FAQ-CA23-11).

Exploited in the wild in a CyberArk environment:

Not to the best of CyberArk's knowledge.

Cyberark Security Bulletin CA23-12

Impact: Exposure of Sensitive Information to an Unauthorized Actor

Jun 21, 2023 · Knowledge Article

Article Total View Count
703

Article Number
000031511

Title
Cyberark Security Bulletin CA23-12

Details
CA23-12

Issued: June 20, 2023

Updated: N/A

Version: 1.0

Severity: High

Score: 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
Privileged Threat Analytics (PTA), Self-hosted	All versions prior to 13.0	

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

Fix Instructions:

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	Download	Documentation
PTA 13.0 or 13.2	No action required		

PTA 12.6 (LTS) and its patches prior to 12.6.6 or older versions	12.6.6	https://www.cyberark.com/CA23-12-PTA-12.6.6 (https://www.cyberark.com/CA23-12-PTA-12.6.6)	Upgrade PTA for 12.6 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PTA/Workflow-Upgrading-PTA.htm)
PTA 12.2 (LTS) and its patches prior to 12.2.11 or older versions	12.2.11	https://www.cyberark.com/CA23-12-PTA-12.2.11 (https://www.cyberark.com/CA23-12-PTA-12.2.11)	Upgrade PTA for 12.2 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PTA/Workflow-Upgrading-PTA.htm)
PTA 11.5 (LTS) and its patches prior to 11.5.16 or older versions	11.5.16	https://www.cyberark.com/CA23-12-PTA-11.5.16 (https://www.cyberark.com/CA23-12-PTA-11.5.16)	Upgrade PTA for 11.5 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PTA/Workflow-Upgrading-PTA.htm)

Temporary mitigation:

There is no temporary mitigation for this bulletin.

For more technical information, see the Technical FAQ (https://cyberark-customers.force.com/s/article/CyberArk-Security-Bulletin-FAQ-CA23-12).

Exploited in the wild in a CyberArk environment:

Not to the best of CyberArk's knowledge.

Cyberark Security Bulletin CA23-13

Potential security bypass on PTA web by an Unauthorized Actor

Jun 20, 2023 · Knowledge Article

Article Total View Count
148

Article Number
000031512

Title
Cyberark Security Bulletin CA23-13

Details
CA23-13

Issued: June 20, 2023

Updated: N/A

Version: 1.0

Severity: High

Score: 7.5

Third Party Publication / CVE: CVE-2023-20860 (https://nvd.nist.gov/vuln/detail/CVE-2023-20860)

Impact: Potential security bypass on PTA web by an Unauthorized Actor

Affected products and versions:

Product	Version(s)	Additional Information
Privileged Threat Analytics (PTA), Self-hosted	PTA 11.5 (LTS) and its patches prior to 11.5.16	

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

Fix Instructions:

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.

Installed version	Patch	Download	Documentation
PTA versions higher than 11.5	No action required		
PTA 11.5 (LTS) and its patches prior to 11.5.16 or older versions	11.5.16	https://www.cyberark.com/CA23-13-PTA-11.5.16 (https://www.cyberark.com/CA23-13-PTA-11.5.16)	Upgrade PTA for 11.5 (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PTA/Workflow-Upgrading-PTA.htm)

Temporary mitigation:

There is no temporary mitigation for this bulletin.

For more technical information, see the Technical FAQ (https://cyberark-customers.force.com/s/article/Cyberark-Security-Bulletin-FAQ-CA23-13).

Exploited in the wild in a CyberArk environment:

Not to the best of CyberArk's knowledge.