Cyberark Security Bulletin CA23-03 Privilege Cloud

A recently identified change in Chrome policy hardening settings caused insufficient hardening of Chrome on the PSM machine.

Mar 20, 2023 · Knowledge Article

Article Number
000030350

Title
Cyberark Security Bulletin CA23-03 Privilege Cloud

Details
Privilege Cloud (SaaS): Lack of hardening values in Privileged Session Manager GPO due to Chrome policy changes

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified change in Chrome policy hardening settings caused insufficient hardening of Chrome on the PSM machine.

Affected Software

All Privilege Cloud Connector versions prior to 12.7.

Detailed Explanation

Usage by Privilege Cloud Connector versions prior to 12.7 of hardening values deprecated by Chrome, instead of the updated values in the GPO provided to Privileged Session Manager, caused insufficient hardening settings of Chrome on the PSM machine. Lack of the adjusted settings might enable PSM to perform operations supported by Chrome that were previously blocked.

Recommendations

CyberArk recommends that all customers using Privilege Cloud Connector versions prior to 12.7 upgrade the Privilege Cloud Connector to the latest available connector version (currently version 13.1) according to the instructions below.

INSTRUCTIONS

1. Download the Privilege Cloud Connector version 13.1 from the CyberArk Marketplace (https://www.cyberark.com/ca23-03-PCloud-13.1).
2. Install the package according to the upgrade instructions (https://www.cyberark.com/PCloud-13.1-Upgrade-Instructions) in our online documentation. Since the fix involves changes in the hardening process, make sure to run the hardening procedure as part of the upgrade.

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects Privileged Session Manager.

Can this vulnerability be exploited by any user?

Any authenticated user that can connect using Chrome through PSM can exploit this vulnerability. An unauthenticated user may be able to exploit this vulnerability if an authenticated user has installed a malicious Chrome extension.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-03-Privilege-Cloud

Article Record Type
Security Bulletin

Cyberark Security Bulletin CA23-03 Self-Hosted

A recently identified change in Chrome policy hardening settings caused insufficient hardening of Chrome on the PSM machine.

Mar 20, 2023 · Knowledge Article

Article Number
000030349

Title
Cyberark Security Bulletin CA23-03 Self-Hosted

Details
Self-Hosted Privilege Access Manager: Lack of hardening values in Privileged Session Manager GPO due to Chrome policy changes

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified change in Chrome policy hardening settings caused insufficient hardening of Chrome on the PSM machine.

Affected Software

All self-hosted Privileged Session Manager versions prior to version 13.0.

Detailed Explanation

Usage by PSM self-hosted versions prior to version 13.0 of hardening values deprecated by Chrome, instead of the updated values in the GPO provided to Privileged Sess insufficient hardening settings of Chrome on the PSM machine. Lack of the adjusted settings might enable PSM to perform operations supported by Chrome that were p

Recommendations

CyberArk recommends that all customers using self-hosted Privileged Session Manager versions prior to version 13.0 patch or upgrade the PSM according to the instruc

INSTRUCTIONS

1. Upgrade your PSM to the applicable patch version below by downloading from the respective link and following the appropriate upgrade instructions https://docs.cyb Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading-the-Privileged-Session-Manager.htm (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm).
2. Run the appropriate hardening procedure for PSM as described in the documentation linked in the table.
3. For in-domain deployments, update the GPO as described in the documentation linked in the table.

Note: The PSM patches are backward compatible with all PAS versions that are within their development period, as per the CyberArk End-of-Life Policy. (https://docs.cyb Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm)

Installed Version	Patch Version	Download link	Documentation
11.5	11.5.15	https://www.cyberark.com/PSM-11.5.15 (https://www.cyberark.com/PSM-11.5.15)	• 11.5 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAthe-PSM.htm) • PSM Hardening Tasks (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Install_PSM_harden.htm) • Hardening 'In Domain' deployment (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Install_PSM_harden.htm#AutomatichardeninginOu
12.2	12.2.10	https://www.cyberark.com/PSM-12.2.10 (https://www.cyberark.com/PSM-12.2.10/)	• 12.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAthe-PSM.htm) • PSM Hardening Tasks (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Install_PSM_harden.htm) • Hardening 'In Domain' deployment (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Install_PSM_harden.htm#HardeningInDomaindeplo
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5 (https://www.cyberark.com/PSM-12.6.5)	• 12.6 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAthe-PSM.htm) • PSM Hardening Tasks (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Install_PSM_harden.htm) • Hardening 'In Domain' deployment (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Install_PSM_harden.htm#HardeningInDomaindeplo

Note: If you use a Chrome version prior to v86 and have never run GPO hardening settings, the Chrome version must be updated before applying the PSM patch.

FREQUENTLY ASKED QUESTIONS (FAQ)

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects Privileged Session Manager.

Can this vulnerability be exploited by any user?

Any authenticated user that can connect using Chrome through PSM can exploit this vulnerability. An unauthenticated user may be able to exploit this vulnerability if an a installed a malicious Chrome extension.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-03-Self-Hosted

Article Record Type
Security Bulletin

Cyberark Security Bulletin CA23-04 Privilege Cloud

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially expose PSMConnect and PSMAdminConnect passwords, in certain configurations, during the PSM installation or upgrade process.

Mar 20, 2023 · Knowledge Article

Article Number
000030352

Title
Cyberark Security Bulletin CA23-04 Privilege Cloud

Details
Privilege Cloud (SaaS): Potential sensitive data exposure in Privileged Session Manager

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially expose PSMConnect and PSMAdminConnect passwords, in certain configurations, during the PSM installation or upgrade process.

Affected Software

All Privilege Cloud Connector versions.

Detailed Explanation

Under certain auditing configurations, the PSMConnect and PSMAdminConnect passwords might be exposed in the Windows event log during PSM installation or upgrade. If there is SIEM system integration, the passwords might be sent to an external system.

Recommendations

CyberArk strongly recommends that all customers using Privilege Cloud Connector versions prior to version 13.1 upgrade Privilege Cloud Connector to v13.1 according to the instructions below. In addition, we strongly recommend that the PSMConnect and PSMAdminConnect passwords are rotated, either by CPM (strongly advised) or manually if CPM is not used. For more details, see Change password (https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-manage-accounts.htm?tocpath=End%20Users%7CManage%20your%20accounts%7C_____0#Changepassword).

Due to the sensitivity of the PSMConnect and PSMAdminConnect credentials, CyberArk strongly recommends, as a security best practice, that these credentials be managed by CPM.

1. Download the Privilege Cloud Connector version 13.1 from the CyberArk Marketplace (https://www.cyberark.com/ca23-04-PCloud-13.1).
2. Install the package according to the upgrade instructions (https://www.cyberark.com/PCloud-13.1-Upgrade-Instructions) in our online documentation.
3. We strongly recommend that the PSMConnect and PSMAdminConnect passwords are rotated, either by CPM (strongly advised) or manually if CPM is not used. For more details, see Change password (https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-manage-accounts.htm?tocpath=End%20Users%7CManage%20your%20accounts%7C_____0#Changepassword).

FREQUENTLY ASKED QUESTIONS (FAQ)

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects the PSM machine.

Can this vulnerability be exploited by any user?

Any user who has privileges to view the event logs on the PSM server or, with SIEM system integration has privileges to view the logs on the SIEM system, can view the sensitive data.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-04-Privilege-Cloud

Article Record Type
Security Bulletin

Cyberark Security Bulletin CA23-04 Self-Hosted

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially expose PSMConnect and PSMAdminConnect passwords, in certain configurations, during the PSM installation or upgrade process.

Mar 20, 2023 · Knowledge Article

Article Number

000030351

Title

Cyberark Security Bulletin CA23-04 Self-Hosted

Details

Self-Hosted Privilege Access Manager: Potential sensitive data exposure in Privileged Session Manager

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially expose PSMConnect and PSMAdminConnect passwords, in certain configurations, during the PSM installation or upgrade process.

Affected Software

All self-hosted Privileged Session Manager versions.

Detailed Explanation

Under certain auditing configurations, the PSMConnect and PSMAdminConnect passwords might be exposed in the Windows event log during PSM installation or upgrade. If there is SIEM system integration, the passwords might be sent to an external system.

Recommendations

CyberArk strongly recommends that all customers using self-hosted Privileged Session Manager versions patch or upgrade the PSM according to the instructions below.

Due to the sensitivity of the PSMConnect and PSMAdminConnect credentials, CyberArk strongly recommends, as a security best practice, that these credentials be managed by CPM. Associate a reconcile account with the platform to ensure successful password rotation. For details, see Configure the PSM users' passwords (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PostInstall_mand.htm#ConfigurethePSMuserspasswords).

Upgrade your PSM to the applicable patch version below by downloading from the respective link and following the appropriate upgrade instructionshttps://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading-the-Privileged-Session-Manager.htm (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm).

Note: The PSM patches are backward compatible with all PAS versions that are within their development period, as per the CyberArk End-of-Life Policy. (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm)

Installed Version	Patch Version	Download link	Documentation
11.5	11.5.15	https://www.cyberark.com/PSM-11.5.15 (https://www.cyberark.com/PSM-11.5.15)	11.5 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
12.2	12.2.10	https://www.cyberark.com/PSM-12.2.10 (https://www.cyberark.com/PSM-12.2.10/)	12.2 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5 (https://www.cyberark.com/PSM-12.6.5)	12.6 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
13.0	13.0.1.	https://www.cyberark.com/PSM-13.0.1 (https://www.cyberark.com/PSM-13.0.1)	13.0 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Upgrading-the-PSM.htm)

FREQUENTLY ASKED QUESTIONS (FAQ)

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects Privileged Session Manager.

Can this vulnerability be exploited by any user?

Any user who has privileges to view the event logs on the PSM server or, with SIEM system integration has privileges to view the logs on the SIEM system, can view the sensitive data.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-04-Self-Hosted

Article Record Type
Security Bulletin

Cyberark Security Bulletin CA23-05 Privilege Cloud

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially cause a denial of service for the PSM service when connecting with certain connection components in certain circumstances.

Mar 20, 2023 · Knowledge Article

Article Number
000030354

Title
Cyberark Security Bulletin CA23-05 Privilege Cloud

Details
Privilege Cloud (SaaS): Potential denial of service (DoS) of Privileged Session Manager

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially cause a denial of service for the PSM service when connecting with certain connection components in certain circumstances.

Affected Software

Privilege Cloud Connector versions 12.5, 12.6, 12.7, and 13.0.

Detailed Explanation

Connecting through PSM using certain connection components that contain certain crafted input can lead to a denial of service of PSM.

Recommendations

CyberArk strongly recommends that all customers using self-hosted Privilege Cloud Connector versions prior to version 13.1 upgrade the Privilege cloud connector to v13.1 according to the instructions below.

INSTRUCTIONS

1. Download the Privilege Cloud Connector version 13.1 from the CyberArk Marketplace (https://www.cyberark.com/ca23-05-PCloud-13.1).
2. Install the package according to the upgrade instructions (https://www.cyberark.com/PCloud-13.1-Upgrade-Instructions) in our online documentation.

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects the PSM machine.

Can this vulnerability be exploited by any user?

A malicious user authenticated to PVWA can exploit the issue.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-05-Privilege-Cloud

Article Record Type
Security Bulletin

Cyberark Security Bulletin CA23-05 Self-Hosted

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially cause a denial of service for the PSM service when connecting with certain connection components in certain circumstances.

Mar 20, 2023 · Knowledge Article

Article Number
000030353

Title
Cyberark Security Bulletin CA23-05 Self-Hosted

Details
Self-Hosted Privilege Access Manager: Potential denial of service (DoS) of Privileged Session Manager

Issued: March 20, 2023

Updated: NA

Version: 1.0

Severity: High

GENERAL INFORMATION

Executive Summary

A recently identified vulnerability in Privileged Session Manager (PSM) can potentially cause a denial of service for the PSM service when connecting with certain connection components in certain circumstances.

Affected Software

Self-hosted Privileged Session Manager versions 12.6 and 13.0.

Detailed Explanation

Connecting through PSM using certain connection components that contain certain crafted input can lead to a denial of service of PSM.

Recommendations

CyberArk strongly recommends that all customers using self-hosted Privileged Session Manager versions 12.6 and 13.0 patch or upgrade the PSM according to the instructions below.

INSTRUCTIONS

Upgrade your PSM to the applicable patch version below by downloading from the respective link and following the appropriate upgrade instructionshttps://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading-the-Privileged-Session-Manager.htm (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm).

Note: The PSM patches are backward compatible with all PAS versions that are within their development period, as per the CyberArk End-of-Life Policy. (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm)

Installed Version	Patch Version	Download link	Documentation
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5 (https://www.cyberark.com/PSM-12.6.5)	12.6 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-PSM.htm)
13.0	13.0.1.	https://www.cyberark.com/PSM-13.0.1 (https://www.cyberark.com/PSM-13.0.1)	13.0 upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Upgrading-the-PSM.htm)

FREQUENTLY ASKED QUESTIONS (FAQ)

Does this vulnerability put the Vault Server at risk?

No, this vulnerability only affects Privileged Session Manager.

Can this vulnerability be exploited by any user?

A malicious user authenticated to PVWA can exploit the issue.

Is there a public exploit for this vulnerability?

CyberArk has not received any information that indicates that this vulnerability has been exploited in any customer environment.

URL Name
Cyberark-Security-Bulletin-CA23-05-Self-Hosted

Article Record Type
Security Bulletin