Cyberark Security Bulletin CA22-21

A recently identified vulnerability in Red Hat Enterprise Linux (RHEL) operating system (OS), used by CyberArk Privileged Threat Analytics (PTA), may in some circumstances enable an attacker to leak information from the PTA Server and may cause a denial of service of the PTA Server. Since all former PTA versions don't support RHEL 8, which includes a repair for this vulnerability, a migration to our newest PTA version 13.0 which supports RHEL 8 is required.

Dec 19, 2022 · Knowledge Article

Article Number

000028213

Title

Cyberark Security Bulletin CA22-21

Details

Security vulnerability in an Operating System used by Privileged Threat Analytics (PTA)
Issued: Dec. 19, 2022
Updated: N/A
Version: 1.0
Severity: High

GENERAL INFORMATION
Executive Summary
A recently identified vulnerability in Red Hat Enterprise Linux (RHEL) operating system (OS), used by CyberArk Privileged Threat Analytics (PTA), may in some circumstances enable an attacker to leak information from the PTA Server and may cause a denial of service of the PTA Server. Since all former PTA versions don't support RHEL 8, which includes a repair for this vulnerability, a migration to our newest PTA version 13.0 which supports RHEL 8 is required.
Affected Software
Privilege Threat Analytics (PTA) prior to version 13.0
Detailed Explanation
Recently, a vulnerability was identified in OS RHEL 7 and consequently in its binary-compatible fork, CentOS 7 (see CVE-2022-1012 (https://nvd.nist.gov/vuln/detail/CVE-2022-1012)), used by CyberArk PTA. This vulnerability may enable an attacker to leak information from the PTA Server and may cause a denial of service of the PTA Server or the PTA Application.
According to the OS vendor (https://access.redhat.com/security/cve/cve-2022-1012), this flaw cannot be repaired in RHEL 7. The fix for this CVE is delivered in RHEL 8 and later.
Recommendations
Since all PTA versions prior to version 13.0 are not able to support RHEL 8 because this will require an architectural change to these PTA versions, to mitigate this vulnerability, CyberArk highly recommends that all customers using PTA prior to version 13.0 migrate the PTA Server to version 13.0, which is supported on RHEL 8 (and its binary-compatible forks Rocky Linux and AlmaLinux), the OS version that includes the fix to the aforementioned vulnerability.
Following security best practices and an upcoming end of life of RHEL 7 and its binary-compatible fork CentOS 7 by their vendor, PTA no longer supports these operating systems. Therefore, all existing PTA versions prior to version 13.0 (including LTS versions) are no longer supported, as they only support RHEL 7.

Note: The migration to PTA version 13.0 should be performed by the customer. Professional Services are not required to perform this migration.

Instructions
To migrate from an existing PTA environment (all PTA versions prior to 13.0) to PTA version 13.0, follow the steps below:

Installed PTA Version	Steps
Below v12.2.6	1. Upgrade your PTA to version 12.2.6, 12.2.7, or 12.6 according to the upgrade instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PTA/Workflow-Upgrading-PTA.htm) in our documentation. The upgrade packages of PTA versions 12.2.6, (https://www.cyberark.com/PTA-12.2.6) 12.2.7 (https://www.cyberark.com/PTA-12.2.7), or 12.6 (https://www.cyberark.com/PTA-12.6) can be downloaded from the Marketplace. 2. Run the migration process according to the migrate instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/Importing-PTA%20to-new-PTA.htm) in our documentation. In high level, the migration process includes the following steps: a. Deploy a new machine with RHEL8.6 (or its binary-compatible forks Rocky Linux and AlmaLinux) OS b. Install PTA version 13.0 according to PTA Server System Requirements (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/System-Requirements-PTA.htm) and the PTA Installation instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/Workflow-Installing-Configuring-Using-PTA.htm) in our documentation. The installation packages of PTA version 13.0 (https://www.cyberark.com/PTA-13.0) can be downloaded from the Marketplace. c. Run the import_PTA_data.sh utility on the new PTA machine to migrate the data from the previous PTA machine to the new one.

v12.2.6 and higher	Run the migration process according to the migrate instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/Importing-PTA%20to-new-PTA.htm) in our documentation. In high level, the migration process includes the following steps: 1. Deploy a new machine with RHEL8.6 (or its binary-compatible forks Rocky Linux and AlmaLinux) OS 2. Install PTA version 13.0 according to PTA Server System Requirements (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/System-Requirements-PTA.htm) and the PTA Installation instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/Workflow-Installing-Configuring-Using-PTA.htm) in our documentation. The installation packages of PTA version 13.0 (https://www.cyberark.com/PTA-13.0) can be downloaded from the Marketplace. 3. Run the import_PTA_data.sh utility on the new PTA machine to migrate the data from the previous PTA machine to the new one.

Please note that as of PTA version 12.6 and above, customers should manage any future updates, including security updates, of the third-party packages on the OS, besides the core third-party dependencies that come with the PTA installation package. For further information see: PTA Server System Requirements. (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/System-Requirements-PTA.htm)

FREQUENTLY ASKED QUESTIONS (FAQ)

Do I need to migrate my PTA Server to a newer version to mitigate this vulnerability?
Yes, the fix for the vulnerability is available on RHEL 8 operating system, which is only supported by PTA version 13.0. Please follow the instructions set forth in this security bulletin.
Note: The migration to PTA version 13.0 should be performed by the customer. Professional Services are not required to perform this migration. If you have questions while migrating, please contact CyberArk Support.
Why is there no patch/upgrade available for an existing PTA version (including LTS versions)?
All PTA versions prior to version 13.0 are not able to support RHEL 8 because this requires an architectural change to these versions, and therefore there is no patch available. To mitigate this vulnerability, a migration of PTA Server to version 13.0, which supports RHEL 8, is required, as further instructed in this security bulletin.

I migrated my PTA to version 13.0. Do I still need to patch/upgrade the rest of the CyberArk components?
No, this vulnerability only affects the PTA Server. I migrated my PTA to version 13.0.

Is it still compatible with the rest of the CyberArk components that were not upgraded?
PTA supports (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PAS%20SysReq/Compatibility_component_versions.htm) all PAM versions. For feature compatibility, see CyberArk Vault / Privileged Access Manager - SelfHosted Compatibility (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PTA/CyberArk-Vault-EPV-Compatibility.htm).

Do I need to upgrade the PTA Agent installed on my Domain Controller?
No, there is no need to upgrade the PTA Agent.

Does this vulnerability put the Vault Server at risk?
No, this vulnerability only affects the PTA Server.

Can any user exploit this vulnerability?
Yes, once specific conditions are met, any user within the organization's network may exploit this vulnerability.

Can this vulnerability be exploited from a remote location?
Yes, the vulnerability may be exploited from any location with a connectivity to the PTA Server within the organization's network.

Is there a public exploit for this vulnerability?
CyberArk has not received any information that indicates that this vulnerability has been publicly exploited in CyberArk products.
Please refer to the following publications of the CVE in RHEL:

• https://nvd.nist.gov/vuln/detail/CVE-2022-1012 (https://nvd.nist.gov/vuln/detail/CVE-2022-1012)
• https://access.redhat.com/security/cve/cve-2022-1012 (https://access.redhat.com/security/cve/cve-2022-1012)

URL Name
Cyberark-Security-Bulletin-CA22-21