Product Vulnerability Management Policy

Updated as of December 22, 2025

1. General

Introduction

As a provider of software security solutions, CyberArk recognizes the vital importance of the security of its products, including the management of vulnerabilities within these products. CyberArk takes a proactive approach to continuously reduce the vulnerabilities in its products and the risks associated with them.

This policy outlines CyberArk's product vulnerability management strategy. It pertains to management of vulnerabilities in CyberArk's products, including third-party components that are embedded within the products, as well as those that are part of CyberArk's Software as a Service (SaaS) cloud environment. It excludes missing product functionalities, as well as platforms and operating systems that CyberArk's products may integrate with, connect to, or be hosted on, that are not distributed as part of CyberArk's offering or are not under CyberArk's control. If a security-related issue is not a vulnerability as defined under this policy, it will not be managed in accordance with this policy. CyberArk may, in its sole discretion, add such an issue to the product's security backlog and prioritize it in accordance with its risk assessment.

This policy applies to vulnerabilities identified after the effective date of this policy. CyberArk may update this policy from time to time in its sole discretion and without notice.

Underlying Assumptions

CyberArk's underlying assumption in its approach to vulnerability management is that the customers' administrators are not careless, willfully negligent, or hostile, and that they administer the products in accordance with the customer's internal security policies and in compliance with the product documentation, including security best practices.

Internal Governance

The vulnerability management process, as set forth in this policy, is overseen by CyberArk's Product Security Office (PSO), which is a team that consists of stakeholders from different departments in CyberArk that are responsible for product security. The PSO is led by CyberArk's CISO and reports to CyberArk's Chief Product and Technology Officer.

2. Proactive Security

Secure Software Development Lifecycle (SSDLC)

CyberArk engages in various proactive processes throughout the course of software development that are designed to prevent the creation of vulnerabilities.

CyberArk follows a Secure Software Development Lifecycle (SSDLC) process based on the Microsoft Secure Development Lifecycle (SDL) that integrates security-related activities into the development process, including well-defined requirement specification, detailed design, security-driven code review, dedicated unit testing and heavy regression testing, as well as robust third-party library management and secure configuration.

CyberArk is also guided by other industry standards, such as those published by the National Institute of Standards and Technology (NIST) and Open Web Application Security Project (OWASP), the CSA Cloud Controls Matrix (CCM) framework, and the STRIDE methodology for threat modeling.

Identification of Vulnerabilities

CyberArk's proactive security strategy includes substantial vulnerability identification processes, both manual and automated, that are designed to enable early discovery of potential vulnerabilities. Such identification activities include, among others, threat modeling, internal and external penetration testing, and security scans, that include software composition analysis, static code analysis, and dynamic scans.

3. Reporting a Suspected Vulnerability

If a customer, partner, or other third party discovers a suspected vulnerability that affects a product, CyberArk encourages them to responsibly disclose the issue to CyberArk and provide the details required to reproduce it. To report a security issue, please contact Engineering Security at product_security@cyberark.com or open a support ticket with CyberArk Support. The relevant team may reach out to the reporter to gather additional details required to recreate the issue. If a vulnerability is confirmed, this policy will take effect immediately.

4. Vulnerability Evaluation

Each vulnerability, whether identified by CyberArk or disclosed to CyberArk by a third party, is evaluated to assess its severity, vulnerable flows, impact, root cause, exploitability level, and the scope of affected products and versions.

CyberArk assesses the security severity rating of identified vulnerabilities based on an industry-accepted methodology, currently CVSS 4.0 (or CVSS 3.1 if needed and appropriate), which takes into consideration the combination of the vulnerability's likelihood, scope, and impact. If CVSS is unsuitable, alternative methodologies may be used. If a vulnerability is identified in a third-party software component that is used in a product, CyberArk will adjust its CVSS score to reflect the impact of the vulnerability in the context of the relevant CyberArk product.

5. Vulnerability Remediation

A remediation of a vulnerability may be provided in one of various methods, including an application-level fix through an updated version or patch, a configuration change (manual or automated), a documentation change, a change to the SaaS infrastructure applied by CyberArk, or any other suitable form.

The remediation may also include temporary mitigation, if available, offering an immediate workaround until the final remediation is applied.

Service Level Objectives (SLO)

SaaS Products

CyberArk endeavors to timely remediate critical and high severity vulnerabilities in its SaaS products by releasing a fix in accordance with their severity. For medium severity vulnerabilities, CyberArk will release a fix in accordance with their risk assessment. All other vulnerabilities will be added to the product backlog. CyberArk will notify customers when such fixes are made available if any customer action is required.

Self-hosted Software

CyberArk endeavors to timely remediate critical and high severity vulnerabilities in its Self-Hosted Software in accordance with their severity. For critical severity vulnerabilities, CyberArk will release a fix to all versions that are within their Development Period, as set forth in the End-of-Life Policy. For high severity vulnerabilities, CyberArk will release a fix that will be included in an upcoming product version, as well as a fix to the latest available version and the Long-Term Support (LTS) versions that are within their Development Period, as set forth in the End-of-Life Policy. For medium severity vulnerabilities, CyberArk will release a fix that will be included in the latest version and in accordance with their risk assessment. All other vulnerabilities will be added to the product backlog. CyberArk will notify customers when such fixes are made available if any customer action is required.

CyberArk may deviate from the foregoing SLOs, pursuant to CyberArk's formal exception process, if additional factors warrant such deviation, subject to approval by the PSO, and in certain cases, additional approval of relevant executives.

6. Verification

Following the completion of remediation activities, and prior to officially closing a vulnerability, a verification phase will be conducted. The verification phase, which is distinct from standard development or QA testing, is designed to confirm that the identified vulnerability has been effectively resolved and that no residual impact or security risk remains. Verification activities leverage appropriate security testing methods and tools to validate the effectiveness of the remediation and are designed to ensure that no related components or functionalities have been adversely affected. A vulnerability may be marked as resolved or closed only after successful completion of this verification phase.

7. Reporting

CyberArk will report a vulnerability to its customers when customers are required to take action to apply the remediation. Reporting of vulnerability-related issues may be via a security bulletin, a release note, a knowledge base article, an in-product notification, or any other appropriate notification method.

To protect the security of CyberArk's customers, reporting of a vulnerability (including disclosure to any individual customer) will only be made once a remediation is made generally available by CyberArk, unless otherwise required by applicable law or regulation.

Definitions and Terminology

For the purpose of this policy, the following terms are used in this document:

- **End-of-Life Policy**: CyberArk's End-of-Life Policy, as updated by CyberArk from time to time, available at End-of-life policy | CyberArk Docs.
- **Product:** CyberArk's Self-Hosted Software and SaaS Products made available by CyberArk to its customers.
- **SaaS Products**: CyberArk's software-as-a-service products, including CyberArk's proprietary software agents and connectors that are to be locally installed by customers for the purpose of interacting with the relevant SaaS Product.
- **Self-Hosted Software**: The self-hosted computer software products licensed to customers by CyberArk.
- **Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST SP 800-53 Rev. 5).
- **Vulnerability Management**: The systematic approach for preventing, identifying, analyzing, classifying, and remediating vulnerabilities.