Product Vulnerability Management Policy

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 includes substantive engineering processes for preventing vulnerabilities from being created, manual and automated activities for early identification of vulnerabilities, and diligent responses to vulnerabilities upon discovery.

This policy outlines CyberArk's product vulnerability management strategy. It pertains solely to management of vulnerabilities in CyberArk's products, including third-party components that are embedded within the products. It excludes platforms and operating systems that the products may integrate with, connect to, or be hosted on, and that are not distributed as part of CyberArk's offering.

CyberArk may update this policy from time to time in its sole discretion without notice.

Underlying Assumptions

CyberArk's underlying assumption to 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 customer's internal security policies and in compliance with the products' documentation, including security best practices.

Definitions and Terminology

For the purpose of this policy, the following terms will have the corresponding meaning set out below.

- "**End-of-Life Policy**" means CyberArk's End-of-Life policy, as updated by CyberArk from time to time, available at https://docs.cyberark.com/Product-Doc/OnlineHelp/Portal/EOL/en/Content/End-Of-LifePolicy.htm
- **"Product"** means CyberArk's Self-Hosted Software and SaaS Products made available by CyberArk to its customers.
- **"SaaS Products"** means CyberArk's software-as-a-service products, including CyberArk's proprietary software agents and connectors that are to be locally installed by customer for the purpose of interacting with the relevant SaaS Product.
- **"Security Gap"** means the lack of a product security functionality or measure, designed to meet security industry best practices.
- **"Self-Hosted Software"** means the self-hosted computer software products licensed to customer by CyberArk.
- **"Vulnerability"** means a flaw that could lead to the compromise of the security of a product.
- **"Vulnerability Management"** means the coordinated and methodical strategy for end-to-end handling of preventing, identifying, analyzing, classifying, and remediating vulnerabilities.

Internal Governance

The vulnerability management process, as set forth in this policy is overseen by the Product Security Office (PSO), a team formed of stakeholders from the different departments in CyberArk responsible for product security. The PSO reports to CyberArk's Chief Product Officer.

2. Proactive Security

Secure Software Development Lifecycle (SSDLC)

CyberArk engages in various proactive processes throughout the course of software development, designed to prevent vulnerabilities from being created.

CyberArk follows an SSDLC process based on the Microsoft Secure Development Lifecycle, integrating 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 guided by industry practices such as Open Web Application Security Project (OWASP), Application Security Verification Standard (ASVS), and CSA Consensus Assessments Initiative Questionnaire (CAIQ), and conducts threat modeling (based on STRIDE methodology).

Identification of Vulnerabilities

CyberArk's proactive security strategy includes substantial vulnerability identification processes designed to enable early discovery of potential vulnerabilities. Such identification activities include, among others, threat modeling, internal and external penetration testing and security scans including 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 the products, CyberArk requests they responsibly disclose the issue to CyberArk and provide the details required to reproduce it. To report a security issue, please contact Product Security at: product_security@cyberark.com. The Product Security team may reach out to the reporter to gather additional details required to recreate the issue. If a vulnerability is confirmed, then 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 (as feasible and appropriate), which takes into consideration the combination of the vulnerability's likelihood, scope and impact. 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 CyberArk product.

Note: If an identified issue falls under the definition of a security gap and not a vulnerability, it will not be managed in accordance with this policy, but instead will be added to the product's proactive security backlog and prioritized accordingly.

5. Vulnerability Remediation

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

The remediation may also include a 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 in accordance with their severity, by releasing a fix. Medium and low severity vulnerabilities will be added to the product roadmap. CyberArk will notify customers when such fixes are made available, if action is required by them.

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. Medium and low severity vulnerabilities will be added to the product roadmap. CyberArk will notify customers when such fixes are made available, if action is required by them.

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

6. 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, release notes, knowledge base article, in-product notification or any other appropriate notification method.

For the protection 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. In addition, the level of detail regarding a vulnerability in any reporting will be limited only to the minimum necessary.