CYBERARK SECURITY VULNERABILITY POLICY

Overview

CyberArk is committed to delivering the best software products and services possible, while demonstrating security best practices and alignment to industry standards.

This document outlines CyberArk's product security vulnerability disclosure policy which was designed to benefit all affected parties.

Policy Goals

- Remediate vulnerabilities in a timely manner.
    - Fixes may be in the form of software change (either as a patch or a scheduled version release), or recommendation for environment changes and 3rd party updates.
- Notify affected customers in a timely manner.
    - Security Bulletins and their delivery channels are governed by CyberArk's Vulnerability Assessment Process.

Vulnerability Assessment Process

A security vulnerability discovered in a CyberArk product, underlying system or embedded third-party library, initiates an assessment and analysis process that may vary depending on the vulnerability characteristics.

- Once a vulnerability has been identified, the CyberArk security team assesses its severity ranking (see Severity Rating Methodology).
- Next, our Security and Product Management teams evaluate the risk and possible mitigations. If needed, the matter is escalated to the Incident Response Team (IRT), which includes our VP of R&D, security advisors, and Product Management representative. The IRT is responsible for defining the action plan for addressing the vulnerability.

Typical activities resulting from the vulnerability assessment include:

- Release a software patch
- Notify affected customers and partners via a Security Bulletin which includes vulnerability details and mitigation information
    - Send emails directly to customers from CyberArk Customer Support
    - Post Security Bulletin names and dates on the CyberArk Website
    - Post Security Bulletins in the CyberArk Technical Community Website

- Apply necessary security enhancements to our product roadmap

Security Severity Rating Methodology

Every discovered vulnerability is individually assessed to quantify its overall security severity rating. The results of this analysis are used to guide the disclosure and the mitigation process.

Severity Rating

CyberArk assesses the security severity rating of identified vulnerabilities based on an industry-accepted methodology (OWASP), which takes into consideration the combination of the vulnerability's probability and impact factors.

Probability Assessment Factors

- Whether the vulnerability is publicly known
- Whether there is a known exploit of the vulnerability
- Whether the system uses the vulnerable component or code
- Whether a privileged account is required to exploit the vulnerability
- Whether the vulnerability can be exploited from a remote location
- Whether the security controls that mitigate the vulnerability are in place.
- Whether an honest user interaction is required for a successful attack to take place.

Impact Assessment Factors

- Confidentiality Impact – Scope of data that may be lost and its sensitivity
- Integrity Impact – Scope of data corruption
- Availability Impact – Level of interruption to the product's services and how vital those services are.
- Loss of Accountability – Can the vulnerability exploit be traced to an individual?

Once Probability and Impact Levels are assessed, the following table is then used to calculate the overall severity rank of the vulnerability:

Overall Security Severity Rate				
Impact	**High**	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	**Medium**	**High**
		Probability		

For additional information, please refer to - https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Vulnerability Response per Severity Rating

CyberArk vulnerability response is determined by the severity rating of each vulnerability.

- **Critical** – Vulnerability is promptly addressed by releasing patches for versions within their End of Development period.
- **High** – Vulnerability is usually addressed in the next scheduled release.
- **Medium / Low** – a security enhancement is added to roadmap and addressed within one of the next releases.

Our policy is to disclose general vulnerability information to our customers once a mitigation or a fix is available, in order to avoid public disclosure that will expose our customers' deployments.

While the mitigation times set forth above constitute targeted goals, it is understood that CyberArk uses reasonable commercial efforts to resolve any vulnerability within the timeframes specified therein.

Vulnerability Response per Severity Rating

We welcome collaboration with our customer base as well as their feedback.

Any challenge to CyberArk's assessment of specific vulnerability should be submitted in written form via a customer's account representative to initiate a discussion. Feedback should include relevant explanations, references and arguments based on the rating methodology presented in this document.

CyberArk will review feedback and may share its decision thereafter. The final decision is up to CyberArk's Security and Product Management team who have the best interest of all parties involved.

Note: This policy is subject to change at any time.