CyberArk Security Vulnerability Policy

Table of Contents

Contents

Overview

As a provider of security software, CyberArk takes security issues very seriously and strives to lead by example. We recognize the importance of collaboration between our researchers and customers and seek to improve the safety of our user community.

This document outlines the security vulnerability policy of CyberArk, in which we exercise the disclosure of security vulnerabilities identified and the way we respond in a manner which is designed to benefit all affected parties.

Policy Goals

- Ensure CyberArk's customers are provided with a high level of protection against the vulnerabilities in their deployments.
- Produce an appropriate fix in a timely manner.

  Depending on the vulnerability, a fix 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.
- Disclosure methods of the vulnerability through appropriate channels to our customer community.

Vulnerability Assessment Process

Upon discovery of a security vulnerability in any of CyberArk's products, underlying systems or embedded 3rd party libraries, a process of assessment and analysis commences and 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 R&D security advisors and Product Management representatives. The IRT is responsible for defining the action plan for addressing the vulnerability which may include one or more of the following actions:
  - Further technical research and analysis of the vulnerability
  - Software patch to address the vulnerability
  - Security Bulletin issued to affected customers, or the entire customer base
  - Security enhancement added to our product roadmap

Security Severity Rating Methodology Every vulnerability that is identified is individually assessed to quantify its overall security severity rating. The results of this analysis are used to determine the appropriate disclosure and mitigation process.

Risk and Severity Rating

CyberArk assesses the security severity rating of identified vulnerabilities based on an industry-accepted methodology (currently CVSS 3.1), which takes into consideration the combination of the vulnerability's probability, scope and impact factors. For additional information, please refer to - https://www.first.org/cvss/calculator/3.1

Probability Assessment Factors

- **Attack Vector** – Does the attacker exploit the vulnerable component via the network stack?
- **Attack Complexity** – Can the attacker exploit the vulnerability at will?
- **Privileged Required** – Must the attacker be authorized to the exploitable component prior to attack?
- **User Interaction** – Does the attacker require some other user to perform the action?

Scope Assessment Factor

- Can the attacker affect component whose authority is different than the vulnerable component?

Impact Assessment Factors

- **Confidentiality Impact** – Can attacker obtain all information from impacted component, or is the disclosed information critical?
- **Integrity Impact** - Can attacker modify all information of impacted component, or is the modified information critical?
- **Availability Impact** – Can attacker completely deny access to the affected component, or is the resource critical?

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

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Security Vulnerability Policy per Risk Rating

CyberArk's response to the vulnerability as provided below is determined by the risk and severity rating that was calculated above..

- **Critical** – Vulnerability is promptly addressed by releasing patches for versions within their End of Development period. Please refer to *CyberArk End of Life Policy* for specific dates per version.
- **High** – Vulnerability is usually addressed in the next scheduled release.
- **Medium / Low** – Security enhancement is added to roadmap and addressed within one of the next releases.

CyberArk's 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 to potential exploits of the vulnerability.

The mitigation times set forth above constitute targeted goals. CyberArk uses reasonable commercial efforts to resolve any vulnerability within the such timeframes.

Challenging CyberArk's Risk Rating

If you believe you have found a vulnerability in one of our products, we ask that you follow responsible disclosure guidelines and contact product_security@cyberark.com and work with us toward a quick resolution to protect our customers.

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

CyberArk will review the feedback and take the appropriate decision based on the principles set forth in this policy.

Note: This policy is subject to change at any time without notice.

Updated as of September 2020