ArcSight Policy for Addressing Vulnerabilities

Policy effective date: October 15, 2013

Revised May 3, 2018

Summary

ArcSight, a product group in the Micro Focus Security Business Unit, is committed to reviewing and addressing reported vulnerabilities in a timely and consistent way. This document outlines ArcSight' s policy for addressing vulnerabilities reported or discovered on any supported ArcSight software or appliance product, the certified operating systems they run on, and any bundled third-party software as applied in the context of an ArcSight product.

Vulnerabilities Policy

ArcSight uses the Common Vulnerability Scoring System (CVSS) version 2.0 to rate the severity of a vulnerability in any supported ArcSight software or appliance product, the certified operating systems they run on, and any embedded third-party software as applied in the context of an ArcSight product, whether the root cause is in the ArcSight code or the embedded third-party component. This system helps ArcSight prioritize which vulnerabilities should be addressed first.

Once a vulnerability has been evaluated for severity and prioritized, ArcSight follows this model to deliver a fix:

Severity	Definition	Release Vehicle
Critical	A critical vulnerability could easily be exploited by a remote unauthenticated attacker and lead to system compromise, such as arbitrary code execution without requiring user interaction (for example, a worm). CVSS rating: 7 – 10	ArcSight will take immediate action to resolve critical severity issues and provide the resolution as a hotfix or patch to the latest released version, if appropriate, and include the fix in the next service pack or major/minor release.
High	High indicates flaws that can easily compromise the confidentiality, integrity, or availability of resources. These vulnerabilities allow local users to gain privileges, allow unauthenticated remote users to view protected resources, allow authenticated remote users to execute arbitrary code, or allow local or remote users to cause a denial of service. CVSS rating: 6 – 7	ArcSight will take immediate action to resolve high severity issues and provide the resolution as a hotfix or patch to the latest released version, if appropriate, and include the fix in the next service pack or major/minor release.
Moderate	Moderate flaws may be more difficult to exploit, or affect unlikely configurations, but could still lead to some compromise of the confidentiality, integrity, or availability of resources.	Depending on the issue, ArcSight will make fixes for moderate severity vulnerabilities in the next appropriate hotfix or patch, if applicable, and

	CVSS rating: 4 – 5	include the fix in the next closest service pack or major/minor release.
Low	Low rated vulnerabilities present a security risk, but are less likely to be exploited because of the circumstances required to exploit them, or where a successful exploit would have minimal consequences. CVSS rating: 0 – 3	ArcSight will evaluate low severity issues case by case. Fixes would be made in the next appropriate patch, if applicable, and included in the next service pack or major/minor release.

For a vulnerability noted in the OS running on an appliance, ArcSight will test the OS fixes provided by the vendor, and deliver an update to the customer in the form of an OS update consisting of one or more OS patches.

For a software product installed on the customer's own hardware, ArcSight recommends which patches available from the OS vendor customers should apply to their OS environments.