VMware External Vulnerability Response and Remediation Policy

VMware works hard to build products and services that our customers trust in the most critical operations of their enterprises. The VMware Security Response Policy explains the process followed by the VMware Security Response Center.

About the VMware Security Response Center

A top priority for VMware is to maintain the trust awarded to us by our customers. We recognize that unless our products meet the highest standards for security, customers will not be able to utilize them with confidence. To achieve this, the VMware Security Response Center maintains a program to identify, respond and address vulnerabilities. This publication:

- Documents our policies for addressing vulnerabilities in VMware enterprise and consumer products (on-premises)
- Describes under what circumstances we will issue a Common Vulnerabilities and Exposures (CVE) identifier and a VMware Security Advisory
- Explains how to report a vulnerability in VMware-maintained code
- Defines terminology used in our publications and corrective actions
- Documents our commitment to safe harbor practices

How to report vulnerabilities

The process of reporting vulnerabilities to the VMware Security Response Center

If you believe you have found a vulnerability in a VMware product or service, please let us know by sending a private email to security@vmware.com. We suggest you use encrypted email to submit your reports. You can find our PGP public key at kb.vmware.com/s/article/1055.

VMware follows responsible vulnerability disclosure guidelines, where the researcher privately reports the newly discovered vulnerability in VMware's products and services directly to VMware. This allows VMware to address the vulnerability in the impacted product and services before any party publicly discloses the vulnerability/exploit details. VMware may credit the researcher following responsible vulnerability disclosure guidelines for vulnerability discovery and reporting. VMware response timelines are dependent on several factors, such as severity, complexity, impact and product lifecycle. VMware will make every effort to publish a fix or a corrective action to customers as follows:

- Critical – Begin work on a fix or a corrective action immediately and provide to customers in the shortest commercially reasonable time.
- Important – Deliver a fix in the next planned maintenance or update release of the product where relevant.
- Moderate, Low – Deliver a fix with the next planned release of the product.

If you are a VMware customer, we advise you create a support request with the VMware Global Support Services team.

Step 1: Receive and acknowledge | Step 2: Triage | Step 3: Investigate | Step 4: Remediate | Step 5: Communicate and credit

Figure 1: The VMware Security Response Center's process for handling suspected vulnerabilities.

Understanding severity and CVEs

VMware severity definitions

VMware publications utilize the industry-standard Common Vulnerability Scoring System (CVSS) in addition to qualitative severity terminology that aligns with the Forum of Incident Response and Security Teams (FIRST) standards. Please note that VMware qualitative ratings may change and do not depend only on the CVSS scoring.

Table 1: Severity ratings and scores

VMware qualitative rating	FIRST qualitative rating	CVSS score
Critical	Critical	9.0–10.0
Important	High	7.0–8.9
Moderate	Medium	4.0–6.9
Low	Low	0.1–3.9
None	None	0.0

Keep up to date on the latest vulnerabilities

VMware Security blog

VMware Security Response Center on Twitter

CVE identifiers

As an approved CVE Numbering Authority (CNA), VMware is authorized to assign CVE identifiers to vulnerabilities affecting products within our distinct, agreed-upon scope.

VMware will issue a CVE identifier for a vulnerability when it meets all the following criteria:

- The vulnerability is the result of unexpected behavior in VMware-maintained code
- The vulnerability results in a measurable confidentiality, integrity or availability compromise
- The vulnerability exists in one or more currently supported VMware products documented in the VMware Product Lifecycle Matrix, or the vulnerability exists in a VMware-maintained open source project that is currently supported

VMware Security Advisories

VMware discloses vulnerabilities in VMware Security Advisories, which include the following information:

- Qualitative severity information
- CVSS scoring
- Impacted product suites that are currently supported
- Vulnerability descriptions
- Currently known attack vectors
- Remediation information
- Workarounds for critical severity vulnerabilities (if possible)
- Notes containing confirmation if exploitation is happening in the wild

Workarounds

VMware defines a workaround as a supported, in-place configuration change that addresses currently known attack vectors for a given vulnerability. VMware will investigate potential workarounds for critical severity vulnerabilities documented in VMware Security Advisories.

Safe harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and VMware will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.