



# CVE-2016-5332

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-5332                                                                                                                |
| State           | PUBLISHED                                                                                                                    |
| Assigner        | mitre                                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                 |
| Published       | 2016-08-31 01:59:16 UTC                                                                                                      |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                      |
| Description     | Directory traversal vulnerability in VMware vRealize Log Insight 2.x and 3.x before 3.6.0 allows remote attackers to read ar |

## Risk And Classification

**Primary CVSS:** v3.0 5.3 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**EPSS:** 0.002400000 probability, percentile 0.473180000 (date 2026-05-17)

**Problem Types:** CWE-22 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 5.3   | MEDIUM   | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 2.0     | nvd@nist.gov | Primary | 5     |          | AV:N/AC:L/Au:N/C:P/I:N/A:N                   |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product              | Version | Update | Edition | Language |
|-------------|--------|----------------------|---------|--------|---------|----------|
| Application | Vmware | Vrealize Log Insight | 2.0     | All    | All     | All      |
| Application | Vmware | Vrealize Log Insight | 2.0.5   | All    | All     | All      |
| Application | Vmware | Vrealize Log Insight | 2.5     | All    | All     | All      |
| Application | Vmware | Vrealize Log Insight | 3.0     | All    | All     | All      |
| Application | Vmware | Vrealize Log Insight | 3.3     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

References

| Reference                                                                                                                 | Source       |
|---------------------------------------------------------------------------------------------------------------------------|--------------|
| VMSA-2016-0011                                                                                                            | af854a3a-211 |
| vRealize Log Insight CVE-2016-5332 Directory Traversal Vulnerability                                                      | af854a3a-211 |
| VMware vRealize Log Insight Lets Remote Users Traverse the Directory to View Files on the Target System - SecurityTracker | af854a3a-211 |
| CVE Program record                                                                                                        | CVE.ORG      |
| NVD vulnerability detail                                                                                                  | NVD          |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)