# CVE-2016-7460

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-7460 |
| **State** | PUBLISHED |
| **Assigner** | vmware |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-12-29 09:59:00 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | The Single Sign-On feature in VMware vCenter Server 5.5 before U3e and 6.0 before U2a and vRealize Automation 6.x bef |

## Risk And Classification

**Primary CVSS:** v3.0 9.1 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.020080000 probability, percentile 0.838280000 (date 2026-05-11)

**Problem Types:** CWE-611 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.0 | nvd@nist.gov | Primary | 9.1 | CRITICAL | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H |
| 2.0 | nvd@nist.gov | Primary | 6.4 | | AV:N/AC:L/Au:N/C:P/I:N/A:P |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Partial

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

### NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Vmware | Vrealize Automation | 6.0.0 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.0.1 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.0.1.1 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.0.1.2 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.1.0 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.1.1 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.2.0 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.2.1 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.2.2 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.2.3 | All | All | All |
| Application | Vmware | Vrealize Automation | 6.2.4 | All | All | All |

### Vendor Declared Affected Products

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

### References

| Reference |
| --- |
| VMware vRealize Automation XML External Entity Processing Flaw in Single Sign-On Function Lets Remote Users Obtain Potentially Sensitiv |
| VMSA-2016-0022 |
| VMware vCenter Server XML External Entity Processing Flaws Let Remote Users Obtain Potentially Sensitive Information or Deny Service - S |
| Multiple VMware Products CVE-2016-7460 XML External Entity Injection Vulnerability |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

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