



# CVE-2016-5763

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

## Summary

|                 |                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-5763                                                                                                     |
| State           | PUBLISHED                                                                                                         |
| Assigner        | microfocus                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                      |
| Published       | 2016-11-15 19:30:01 UTC                                                                                           |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                           |
| Description     | Vulnerability in Novell Open Enterprise Server (OES2015 SP1 before Scheduled Maintenance Update 10992, OES2015 be |

## 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:H/A:N

**EPSS:** 0.010340000 probability, percentile 0.774950000 (date 2026-05-10)

**Problem Types:** CWE-254 | unauthorized file access and modification

| 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:H/A:N |
| 2.0     | nvd@nist.gov | Primary | 6.4   |          | AV:N/AC:L/Au:N/C:P/I:P/A:N                   |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                     | Version | Update | Edition | Language |
|-------------|--------|-----------------------------|---------|--------|---------|----------|
| Application | Novell | Open Enterprise Server 11   | All     | sp2    | All     | All      |
| Application | Novell | Open Enterprise Server 11   | All     | sp3    | All     | All      |
| Application | Novell | Open Enterprise Server 2015 | All     | All    | All     | All      |
| Application | Novell | Open Enterprise Server 2015 | All     | sp1    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product                                   | Version                                            | Platforms     |
|--------|--------|-------------------------------------------|----------------------------------------------------|---------------|
| CNA    | Na     | Novell Open Enterprise Server 11 And 2015 | affected Novell Open Enterprise Server 11 and 2015 | Not specified |

References

| Reference                                                                        | Source                               | Link                     |
|----------------------------------------------------------------------------------|--------------------------------------|--------------------------|
| Downloads - September 2016 Update - OES 2015 10990                               | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">download</a> |
| Novell Open Enterprise Server CVE-2016-5763 Remote Security Bypass Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.se</a>   |
| Downloads - September 2016 Update - OES 2015-SP1 10992                           | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">download</a> |
| Downloads - September 2016 OES11 SP3 Scheduled Maintenance Update 10991          | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">download</a> |
| Downloads - September 2016 OES 11 SP2 Scheduled Maintenance Update 10989         | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">download</a> |
| CVE Program record                                                               | CVE.ORG                              | <a href="#">www.cve</a>  |

|                                                                      |        |          |
|----------------------------------------------------------------------|--------|----------|
| CVE Program Records                                                  | CVE ID | https:// |
| NVD vulnerability detail                                             | NVD    | nvd.nist |
| <div></div>                                                          |        |          |
| 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](#)