



CVE-2014-0598

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0598
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-18 17:55:00 UTC
Updated	2020-02-24 14:15:00 UTC
Description	Directory traversal vulnerability in iPrint in Novell Open Enterprise Server (OES) 11 SP1 before Maintenance Update 9151 c

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Novell	Open Enterprise Server	11.0	sp1	All	All
Operating System	Novell	Open Enterprise Server	11.0	sp1	All	All

References

Reference	Source
Support Patches released for Open Enterprise Server 11 Support Pack 1 (OES11 SP1).	CONFIR
Security Advisory SA59113 - Novell Open Enterprise Server Cross-Site Scripting and Directory Traversal Vulnerabilities - Secunia	SECUNIA
Access Denied	CONFIR
Novell Open Enterprise Server CVE-2014-0598 Unspecified Directory Traversal Vulnerability	BID
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](#).

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