CVE-2015-0779

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

Summary

CVE	CVE-2015-0779
State	PUBLISHED
Assigner	microfocus
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-07 23:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Directory traversal vulnerability in UploadServlet in Novell ZENworks Configuration Management (ZCM) 10 and 11 before 1

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-22 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Zenworks Configuration Management	11	All	All	All

Application	Novell	Zenworks Configuration Management	11	sp1	All	All
Application	Novell	Zenworks Configuration Management	11.2	All	All	All
Application	Novell	Zenworks Configuration Management	11.2.1	All	All	All
Application	Novell	Zenworks Configuration Management	11.2.2	All	All	All
Application	Novell	Zenworks Configuration Management	11.2.3	All	All	All

Vendor Declared Affected Products

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

References

Reference
Support | ZENworks Configuration Management Security Announcement: CVE-2015-0779 Remote code execution via file upload and director
Create exploit for CVE-2015-0779 by pedrib · Pull Request #5096 · rapid7/metasploit-framework · GitHub
raw.githubusercontent.com/pedrib/PoC/master/generic/zenworks_zcm_rce.txt
Novell ZENworks Configuration Management - Arbitrary File Upload (Metasploit) - Java remote Exploit
Full Disclosure: [CVE-2015-0779]: Novell ZenWorks Configuration Management remote code execution
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.