

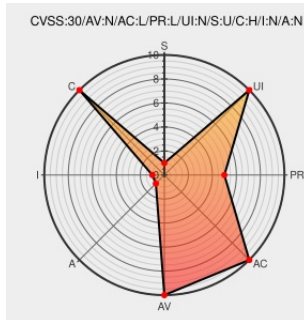


CVE-2017-16591

Published on: 01/22/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16591

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Enterprise Manager](#) from [Netgain-systems](#) contain the following vulnerability:

This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of NetGain Systems Enterprise Manager 7.2.699 build 1001. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the

org.apache.jsp.u.jsp.restore.download_005fdo_jsp servlet, which listens on TCP port 8081 by default. When parsing the filename parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of Administrator. Was ZDI-CAN-5100.

CVE-2017-16591 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **NetGain Systems - NetGain Systems Enterprise Manager** version **7.2.699 build 1001**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Zero Day Initiative	Third Party Advisory VDB Entry zerodayinitiative.com text/html	 MISC zerodayinitiative.com/advisories/ZDI-17-956

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgain-systems	Enterprise Manager	7.2.699	All	All	All
Application	Netgain-systems	Enterprise Manager	7.2.699	All	All	All

cpe:2.3:a:netgain-systems:enterprise_manager:7.2.699:*****.*.*.*

cpe:2.3:a:netgain-systems:enterprise_manager:7.2.699:*****.*.*.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →