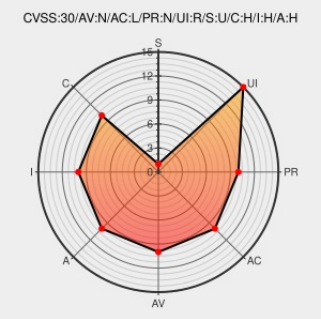
CVE-2017-16590

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

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16590

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 bypass authentication on vulnerable installations of NetGain Systems Enterprise Manager 7.2.699 build 1001. User interaction is required to exploit this vulnerability. The specific flaw exists within the MainFilter servlet. The issue results from the lack of proper string matching inside the doFilter method. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of Administrator. Was ZDI-CAN-5099.

CVE-2017-16590 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

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

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Zero Day Initiative	Third Party Advisory VDB Entry zerodayinitiative.com text/html	MISC zerodayinitiative.com/advisories/ZDI-17-955

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→