



CVE-2016-1524

Published on: 02/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1524

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

Certain versions of [Prosafe Network Management Software 300](#) from [Netgear](#) contain the following vulnerability:

Multiple unrestricted file upload vulnerabilities in NETGEAR Management System NMS300 1.5.0.11 and earlier allow remote attackers to execute arbitrary Java code by using (1) fileUpload.do or (2) lib-1.0/external/flash/fileUpload.do to upload a JSP file, and then accessing it via a direct request for a /null URI.

CVE-2016-1524 has been assigned by cert@cert.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.6 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **8.3 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160204 [CERT 777024 / CVE-2016-1524/5]: RCE and file download in Netgear NMS300

Full Disclosure: [CERT 777024 / CVE-2016-1524/5]: RCE and file download in Netgear NMS300	seclists.org text/html	 FULLDISC 20160204 [CERT 777024 / CVE-2016-1524/5]: RCE and file download in Netgear NMS300
NETGEAR NMS300 ProSafe Network Management System - Multiple Vulnerabilities - Hardware webapps Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 39412
Vulnerability Note VU#777024 - Netgear Management System NMS300 contains arbitrary file upload and path traversal vulnerabilities	Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#777024
Netgear Pro NMS 300 Code Execution / File Download ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135618/Netgear-Pro-NMS-300-Code-Execution-File-Download.html

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	Netgear	Prosafe Network Management Software 300	All	All	All	All
cpe:2.3:a:netgear:prosafe_network_management_software_300:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)