



# CVE-2018-14665

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

## Summary

<b>CVE</b>	CVE-2018-14665
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-10-25 20:29:00 UTC
<b>Updated</b>	2019-10-22 23:15:00 UTC
<b>Description</b>	A flaw was found in xorg-x11-server before 1.20.3. An incorrect permission check for -modulepath and -logfile options wher

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">X.org</a>	<a href="#">Xorg-server</a>	All	All	All	All
Application	<a href="#">X.org</a>	<a href="#">Xorg-server</a>	All	All	All	All

## References

### Reference

Software [in] Security: CVE-2018-14665 : Xorg X Server Vulnerabilities

xorg-x11-server < 1.20.1 - Local Privilege Escalation - Linux local Exploit

Xorg X11 Server SUID modulepath Privilege Escalation ≈ Packet Storm

xorg-x11-server 1.20.3 - Privilege Escalation - OpenBSD local Exploit

Debian -- Security Information -- DSA-4328-1 xorg-server

xorg-x11-server < 1.20.3 - Local Privilege Escalation - Multiple local Exploit

X.Org Command Line Validation Flaw Lets Remote Authenticated Users Gain Elevated Privileges and Delete Arbitrary Files - SecurityTracker

Xorg X11 Server (AIX) - Local Privilege Escalation - AIX local Exploit

X.Org X Server CVE-2018-14665 Multiple Local Privilege Escalation Vulnerability

Xorg X11 Server Local Privilege Escalation ≈ Packet Storm

1637761 – (CVE-2018-14665) CVE-2018-14665 xorg-x11-server: Incorrect permission check in Xorg X server allows for privilege escalation

Xorg X11 Server - SUID privilege escalation (Metasploit) - Multiple local Exploit

xorg-x11-server < 1.20.3 (Solaris 11) - 'inittab Local Privilege Escalation - Solaris local Exploit

Red Hat Customer Portal

X.Org X Server: Privilege escalation (GLSA 201810-09) — Gentoo security

X.Org security advisory: October 25, 2018

Disable -logfile and -modulepath when running with elevated privileges (50c0cf88) · Commits · xorg / xserver · GitLab

USN-3802-1: X.Org X server vulnerability | Ubuntu security notices

xorg-x11-server < 1.20.3 - 'modulepath' Local Privilege Escalation - Multiple local Exploit

Disable -logfile and -modulepath when running with elevated privileges (8a59e3b7) · Commits · xorg / xserver · GitLab

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

500824 Alpine Linux Security Update for xorg-server

© [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](#)**