



CVE-2016-4446

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

Summary

CVE	CVE-2016-4446
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-11 18:59:00 UTC
Updated	2017-04-17 13:29:00 UTC
Description	The allow_execstack plugin for setroubleshoot allows local users to execute arbitrary commands by triggering an execstack

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Setroubleshoot Project	Setroubleshoot	All	All	All	All

References

Reference	Source
SETroubleShoot allow_execmod Plugin Lets Local Users Obtain Root Privileges - SecurityTracker	SEC
Red Hat Customer Portal	RED
1339250 – (CVE-2016-4446) CVE-2016-4446 setroubleshoot-plugins: insecure commands.getoutput use in the allow_execstack plugin	COI
oss-sec: Re: SELinux troubles	MLI
Red Hat Customer Portal	RED

plugins: Use subprocess.check_output() with a sequence of program arg... · fedora-selinux/setroubleshoot@eaccf4c · GitHub	COI
setroubleshoot-plugins CVE-2016-4446 Local Arbitrary Code Execution Vulnerability	BID
CVE Program record	CVE
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)