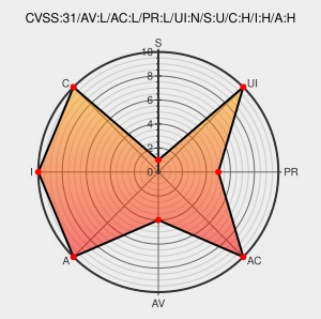
CVE-2016-5425

Published on: 10/13/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:24:00 PM UTC

CVE-2016-5425

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tomcat from Apache contain the following vulnerability:

The Tomcat package on Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, and possibly other Linux distributions uses weak permissions for /usr/lib/tmpfiles.d/tomcat.conf, which allows local users to gain root privileges by leveraging membership in the tomcat group.

CVE-2016-5425 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2046
oss-security - CVE-2016-5425 - Apache	Mailing List	MLIST [oss-security] 20161010 CVE-2016-5425 - Apache

oss-security - CVE-2016-5425 - Apache Tomcat packaging on RedHat-based distros - Root Privilege Escalation (affecting CentOS, Fedora, OracleLinux, RedHat etc.)	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20161010 CVE-2016-5425 - Apache Tomcat packaging on RedHat-based distros - Root Privilege Escalation (affecting CentOS, Fedora, OracleLinux, RedHat etc.)
Apache Tomcat 8/7/6 (RedHat-Based Distros) - Privilege Escalation	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 40488
1362545 – (CVE-2016-5425) CVE-2016-5425 tomcat: Local privilege escalation via systemd-tmpfiles service	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1362545
Pony Mail!	lists.apache.org text/html	MLIST [activemq-issues] 20190925 [jira] [Created] (AMQ-7310) Security Vulnerabilities in Tomcat-websocket-api.jar
Apache Tomcat Weak Configuration File Permissions on Red Hat-based Systems Lets Local Users Obtain Root Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1036979
Oracle Linux Bulletin - October 2016	Third Party Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2016-3090545.html
Apache Tomcat CVE-2016-5425 Insecure File Permissions Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 93472
CVE-2016-5425 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-5425
Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425	Exploit Third Party Advisory legalhackers.com text/html	MISC legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425.html
	legalhackers.com text/plain	MISC legalhackers.com/advisories/Tomcat-RedHat-based-Root-Privilege-Escalation-Exploit.txt
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2046
Oracle Critical Patch Update - October 2019	Third Party Advisory www.oracle.com text/html	MISC www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
Apache Tomcat 8 / 7 / 6 Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/139041/Apache-Tomcat-8-7-6-Privilege-Escalation.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	Apache	Tomcat	-	All	All	All
Application	Apache	Tomcat	-	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	7	-	All	All
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 Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All

Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	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

cpe:2.3:a:apache:tomcat:-:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:-:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomcat:-:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.1:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.2:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.3:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.1:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.2:*:*:*:*:*:*:*

cpe:2.3:a:oracle:instantis_enterprisetrack:17.3:*:*:*:*:*:*:*

cpe:2.3:o:oracle:linux:7:-:*:*:*:*:*:*:

cpe:2.3:o:oracle:linux:7:-:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.3:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.7:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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