



CVE-2018-1336

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

Summary

CVE	CVE-2018-1336
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-02 14:29:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	An improper handling of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the dec

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All
Application	Apache	Tomcat	8.0.0	rc4	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.0	rc6	All	All
Application	Apache	Tomcat	8.0.0	rc7	All	All
Application	Apache	Tomcat	8.0.0	rc8	All	All
Application	Apache	Tomcat	8.0.0	rc9	All	All
Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All
Application	Apache	Tomcat	9.0.0	m16	All	All

Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All
Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m22	All	All
Application	Apache	Tomcat	9.0.0	m23	All	All
Application	Apache	Tomcat	9.0.0	m24	All	All
Application	Apache	Tomcat	9.0.0	m25	All	All
Application	Apache	Tomcat	9.0.0	m26	All	All
Application	Apache	Tomcat	9.0.0	m27	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All
Application	Apache	Tomcat	9.0.0	milestone10	All	All
Application	Apache	Tomcat	9.0.0	milestone11	All	All
Application	Apache	Tomcat	9.0.0	milestone12	All	All
Application	Apache	Tomcat	9.0.0	milestone13	All	All
Application	Apache	Tomcat	9.0.0	milestone14	All	All
Application	Apache	Tomcat	9.0.0	milestone15	All	All
Application	Apache	Tomcat	9.0.0	milestone16	All	All
Application	Apache	Tomcat	9.0.0	milestone17	All	All
Application	Apache	Tomcat	9.0.0	milestone18	All	All
Application	Apache	Tomcat	9.0.0	milestone19	All	All
Application	Apache	Tomcat	9.0.0	milestone20	All	All
Application	Apache	Tomcat	9.0.0	milestone21	All	All
Application	Apache	Tomcat	9.0.0	milestone22	All	All
Application	Apache	Tomcat	9.0.0	milestone23	All	All
Application	Apache	Tomcat	9.0.0	milestone24	All	All
Application	Apache	Tomcat	9.0.0	milestone25	All	All
Application	Apache	Tomcat	9.0.0	milestone26	All	All
Application	Apache	Tomcat	9.0.0	milestone27	All	All
Application	Apache	Tomcat	9.0.0	milestone9	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All

Application	Apache	Tomcat	8.0.0	rc4	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.0	rc6	All	All
Application	Apache	Tomcat	8.0.0	rc7	All	All
Application	Apache	Tomcat	8.0.0	rc8	All	All
Application	Apache	Tomcat	8.0.0	rc9	All	All
Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All
Application	Apache	Tomcat	9.0.0	m16	All	All
Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All
Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m22	All	All
Application	Apache	Tomcat	9.0.0	m23	All	All
Application	Apache	Tomcat	9.0.0	m24	All	All
Application	Apache	Tomcat	9.0.0	m25	All	All
Application	Apache	Tomcat	9.0.0	m26	All	All
Application	Apache	Tomcat	9.0.0	m27	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	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 Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	3.0.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	3.0.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	5.0.0	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache.org
USN-3723-1: Tomcat vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Pony Mail!		lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!	MLIST	lists.apache.org
myF5		support.f5.com
Pony Mail!	MLIST	lists.apache.org
Apache Tomcat Overflow in UTF-8 Decoder Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com

Pony Mail!		lists.apache.org
[SECURITY] [DLA 1491-1] tomcat8 security update	MLIST	lists.debian.org
Pony Mail!	MLIST	lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
July 2018 Apache Tomcat Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!	MLIST	lists.apache.org
Apache Tomcat CVE-2018-1336 Denial of Service Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	access.redhat.com
support.f5.com/csp/article/K73008537	CONFIRM	support.f5.com
Pony Mail!		lists.apache.org
[SECURITY] CVE-2018-1336 Apache Tomcat - Denial of Service	MLIST	mail-archives.us.apache.org
Pony Mail!		lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.com

Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Debian -- Security Information -- DSA-4281-1 tomcat8	DEBIAN	www.debian.org
Pony Mail!	MLIST	lists.apache.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981003 Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-m59c-jpc8-m2x4)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report