CVE-2020-13936

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13936
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-10 08:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands wi

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Velocity Engine	All	All	All	All
Application	Apache	Wss4j	2.3.1	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Oracle	Banking Deposits And Lines Of Credit Servicing	2.12.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.10.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.12.0	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.6.2	All	All	All
Application	Oracle	Banking Enterprise Default Management	2.7.1	All	All	All
Application	Oracle	Banking Enterprise Default Management	All	All	All	All
Application	Oracle	Banking Loans Servicing	2.12.0	All	All	All
Application	Oracle	Banking Party Management	2.7.0	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Banking Platform	2.7.1	All	All	All
Application	Oracle	Banking Platform	All	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All	All	All
Application	Oracle	Communications Network Integrity	7.3.6	All	All	All
Application	Oracle	Hospitality Token Proxy Service	19.2	All	All	All

Application	Oracle	Retail Integration Bus	19.0.1	All	All	All
Application	Oracle	Retail Order Broker	16.0	All	All	All
Application	Oracle	Retail Service Backbone	19.0.1	All	All	All
Application	Oracle	Retail Xstore Office Cloud Service	16.0.6	All	All	All
Application	Oracle	Retail Xstore Office Cloud Service	17.0.4	All	All	All
Application	Oracle	Retail Xstore Office Cloud Service	18.0.3	All	All	All
Application	Oracle	Retail Xstore Office Cloud Service	19.0.2	All	All	All
Application	Oracle	Retail Xstore Office Cloud Service	20.0.1	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.1.1	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.2.2	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.3.1	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advis
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	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	
oss-security - CVE-2020-13936: Velocity Sandbox Bypass	MLIST	www.openwall.com	Mailing List, Third Party A
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
Pony Mail!	CONFIRM	lists.apache.org	Mailing List, Vendor Advis
Pony Mail!	MLIST	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!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advis
Pony Mail!	MLIST	lists.apache.org	Mailing List, Patch, Vendo
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	
Apache Velocity: Multiple vulnerabilities (GLSA 202107-52) — Gentoo security	GENTOO	security.gentoo.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
[SECURITY] [DLA 2595-1] velocity security update	MLIST	lists.debian.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Alvaro Munoz pwntester@github.com of Github Security Labs and was originally reported as GHSL-2020-048.

Legacy QID Mappings

- 174799 SUSE Enterprise Linux Security update for velocity (SUSE-SU-2021:0800-1)
- 178493 Debian Security Update for velocity (DLA 2595-1)
- 199646 Ubuntu Security Notification for Velocity Engine Vulnerability (USN-6281-1)
- 239353 Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.3.7 (RHSA-2021:2048)
- 239354 Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.3.7 (RHSA-2021:2047)

239355 Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.3.7 (RHSA-2021:2046)

239652 Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.4.1 (RHSA-2021:3658)

239653 Red Hat Update for Red Hat JBoss Enterprise Application Platform 7.4.1 (RHSA-2021:3656)

352484 Amazon Linux Security Advisory for velocity: ALAS2-2021-1690

670217 EulerOS Security Update for velocity (EulerOS-SA-2021-1858)

670409 EulerOS Security Update for velocity (EulerOS-SA-2021-1990)

670475 EulerOS Security Update for velocity (EulerOS-SA-2021-2233)

670679 EulerOS Security Update for velocity (EulerOS-SA-2021-2437)

710043 Gentoo Linux Apache Velocity Multiple Vulnerabilities (GLSA 202107-52)

750303 OpenSUSE Security Update for velocity (openSUSE-SU-2021:0447-1)

753357 SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2022:3397-1)