CVE-2009-0217

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-0217
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-14 23:30:00 UTC
Updated	2018-10-12 21:49:00 UTC
Description	The design of the W3C XML Signature Syntax and Processing (XMLDsig) recommendation, as implemented in products inc

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server	6.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.5	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.7	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.9	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	fp17	All

Application	Ibm	Websphere Application Server	6.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.10	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.12	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.14	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.16	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.18	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.19	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.20	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.21	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.22	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.23	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.24	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.25	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.28	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.29	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.30	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.31	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.32	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.33	All	All	All
Application	Ibm	Websphere Application Server	6.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.10	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.11	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.12	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.13	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.14	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.15	All	All	All

Application	Ibm	Websphere Application Server	6.1.0.16	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.18	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.19	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.20	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.22	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.4	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.6	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.8	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.9	All	All	All
Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.5	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.7	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.9	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	fp17	All

Application	Ibm	Websphere Application Server	6.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.10	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.12	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.14	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.16	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.18	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.19	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.20	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.21	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.22	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.23	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.24	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.25	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.28	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.29	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.30	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.31	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.32	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.33	All	All	All
Application	Ibm	Websphere Application Server	6.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.10	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.11	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.12	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.13	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.14	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.15	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.16	All	All	All

Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.18	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.19	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.20	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.22	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.4	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.6	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.8	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.9	All	All	All
Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Mono Project	Mono	1.2.1	All	All	All
Application	Mono Project	Mono	1.2.2	All	All	All
Application	Mono Project	Mono	1.2.3	All	All	All
Application	Mono Project	Mono	1.2.4	All	All	All
Application	Mono Project	Mono	1.2.5	All	All	All
Application	Mono Project	Mono	1.2.6	All	All	All
Application	Mono Project	Mono	1.9	All	All	All
Application	Mono Project	Mono	2.0	All	All	All
Application	Mono Project	Mono	1.2.1	All	All	All
Application	Mono Project	Mono	1.2.2	All	All	All
Application	Mono Project	Mono	1.2.3	All	All	All
Application	Mono Project	Mono	1.2.4	All	All	All
Application	Mono Project	Mono	1.2.5	All	All	All
Application	Mono Project	Mono	1.2.6	All	All	All
Application	Mono Project	Mono	1.9	All	All	All
Application	Mono Project	Mono	2.0	All	All	All
Application	Oracle	Application Server	10.1.2.3	All	All	All
Application	Oracle	Application Server	10.1.3.4	All	All	All

Application	Oracle	Application Server	10.1.4.3im	All	All	All
Application	Oracle	Application Server	10.1.2.3	All	All	All
Application	Oracle	Application Server	10.1.3.4	All	All	All
Application	Oracle	Application Server	10.1.4.3im	All	All	All
Application	Oracle	Bea Product Suite	10.0	mp1	All	All
Application	Oracle	Bea Product Suite	10.3	All	All	All
Application	Oracle	Bea Product Suite	8.1	sp6	All	All
Application	Oracle	Bea Product Suite	9.0	All	All	All
Application	Oracle	Bea Product Suite	9.1	All	All	All
Application	Oracle	Bea Product Suite	9.2	mp3	All	All
Application	Oracle	Bea Product Suite	10.0	mp1	All	All
Application	Oracle	Bea Product Suite	10.3	All	All	All
Application	Oracle	Bea Product Suite	8.1	sp6	All	All
Application	Oracle	Bea Product Suite	9.0	All	All	All
Application	Oracle	Bea Product Suite	9.1	All	All	All
Application	Oracle	Bea Product Suite	9.2	mp3	All	All
Application	Oracle	Weblogic Server Component	10.0	mp1	All	All
Application	Oracle	Weblogic Server Component	10.3	All	All	All
Application	Oracle	Weblogic Server Component	8.1	sp6	All	All
Application	Oracle	Weblogic Server Component	9.0	All	All	All
Application	Oracle	Weblogic Server Component	9.1	All	All	All
Application	Oracle	Weblogic Server Component	9.2	mp3	All	All
Application	Oracle	Weblogic Server Component	10.0	mp1	All	All
Application	Oracle	Weblogic Server Component	10.3	All	All	All
Application	Oracle	Weblogic Server Component	8.1	sp6	All	All
Application	Oracle	Weblogic Server Component	9.0	All	All	All
Application	Oracle	Weblogic Server Component	9.1	All	All	All
Application	Oracle	Weblogic Server Component	9.2	mp3	All	All

References

Reference
55895
[SECURITY] Fedora 11 Update: xmlsec1-1.2.12-1.fc11
511915 – (CVE-2009-0217) CVE-2009-0217 xmlsec1, mono, xml-security-c, xml-security-1.3.0-1jpp.ep1.*: XMLDsig HMAC-based signatures
Apache XML Security HMAC Truncation Spoofing - Secunia Advisories - Vulnerability Information - Secunia.com
rhn.redhat.com | Red Hat Support

Errata for XML Signature 2nd Edition

Repository / Oval Repository

47527 – XML signature HMAC truncation authentication bypass

Red Hat update for java-1.6.0-openjdk - Secunia Advisories - Vulnerability Information - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IETF and W3C XML Digital Signature Specification HMAC Truncation Authentication Bypass Vulnerability

USN-826-1: Mono vulnerabilities | Ubuntu security notices

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

rhn.redhat.com | Red Hat Support

Repository / Oval Repository

[SECURITY] Fedora 10 Update: xmlsec1-1.2.12-1.fc10

XML Security Library

Security Advisory SA60799 - Gentoo openoffice Multiple Vulnerabilties - Secunia

rhn.redhat.com | Red Hat Support

OpenOffice.org 3 Multiple Vulnerabilities - Advisories - Community

IBM PK80596: Possible security exposure with XML digital signature - United States

269208

Ubuntu update for openoffice.org - Advisories - Community

Debian -- Security Information -- DSA-1995-1 openoffice.org

Fedora update for java-1.6.0-openjdk - Secunia Advisories - Vulnerability Information - Secunia.com

Sign in · GitLab

XML Security Library XML Signature HMAC Truncation Spoofing - Secunia Advisories - Vulnerability Information - Secunia.com

[SECURITY] Fedora 11 Update: java-1.6.0-openjdk-1.6.0.0-27.b16.fc11

Oracle Critical Patch Update Advisory - October 2009

OpenOffice.org 2 Multiple Vulnerabilities - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

CVE-2009-0217

APPLE-SA-2009-09-03-1 Java for Mac OS X 10.5 Update 5

Security

#125136-16: Obsoleted by: 125136-17 JavaSE for business 6: update 15 patch (equivalent to JDK 6u15)

Support

rhn.redhat.com | Red Hat Support

Advisories | Mandriva

55907

Microsoft Security Bulletin MS10-041 - Important | Microsoft Docs

SecurityTracker.com Archives - Java Runtime Environment (JRE) XML Digital Signature Flaw May Let Remote Users Bypass Authentication

rhn.redhat.com | Red Hat Support

Sun Java JDK / JRE XML Signature HMAC Truncation Spoofing - Secunia Advisories - Vulnerability Information - Secunia.com

About Secunia Research | Flexera

Sign in · GitLab

US-CERT Vulnerability Note VU#466161

Oracle Open Office Multiple Vulnerabilities - Advisories - Community

HMAC truncation in XML Signature: When Alice didn't look. - W3C Blog

[security-announce] SUSE Security Announcement: OpenOffice.org (SUSE-SA:

US-CERT Technical Cyber Security Alert TA10-159B -- Microsoft Updates for Multiple Vulnerabilities

US-CERT Technical Cyber Security Alert TA09-294A -- Oracle Updates for Multiple Vulnerabilities

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Ubuntu update for mono - Secunia Advisories - Vulnerability Information - Secunia.com

SecurityTracker.com Archives - Oracle Application Server Bugs Let Remote Users Modify Data

Gentoo Linux Documentation -- OpenOffice, LibreOffice: Multiple vulnerabilities

Red Hat update for java-1.6.0-ibm - Secunia Advisories - Vulnerability Information - Secunia.com

Red Hat update for java-1.6.0-sun - Secunia Advisories - Vulnerability Information - Secunia.com

Oracle Products Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

IBM Possible security exposure with XML digital signature with IBM WebSphere Application Server (PK80596 and PK80627) - United States

Sun Microsystems, Inc. Information for VU#466161

RSA Products XML Signature HMAC Truncation Spoofing - Secunia Advisories - Vulnerability Information - Secunia.com

IBM PK80627; Possible security exposure with XML digital signature. - United States

[security-announce] SUSE Security Announcement: IBM Java 6 (SUSE-SA:2009

rhn.redhat.com | Red Hat Support

'[security bulletin] HPSBUX02476 SSRT090250 rev.1 - HP-UX Running Java, Remote Increase in Privilege,' - MARC

Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Apache-SVN] Revision 794013

IBM WebSphere Application Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

Oracle Critical Patch Update Pre-Release Announcement - October 2010

SecurityTracker.com Archives - WebLogic Server Bugs Let Remote Users Gain Access and Modify Data and Deny Service

RSA Security, Inc. Information for VU#466161

Oracle Critical Patch Update Advisory - July 2009

1020710

SUSE update for OpenOffice_org - Secunia.com

SUSE update for OpenOffice_org - Secunia.com
Bug 47526 – XML signature HMAC truncation authentication bypass
#263429: A Security Vulnerability With Verifying HMAC-based XML Digital Signatures in the XML Digital Signature Implementation Included W
USN-903-1: OpenOffice.org vulnerabilities | Ubuntu
[SECURITY] Fedora 10 Update: java-1.6.0-openjdk-1.6.0.0-20.b16.fc10
HP-UX update for JRE / JDK - Secunia Advisories - Vulnerability Information - Secunia.com
Mono XML Signature HMAC Truncation Spoofing - Secunia Advisories - Vulnerability Information - Secunia.com
rhn.redhat.com | Red Hat Support
Repository / Oval Repository
Vulnerabilities - Mono
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.