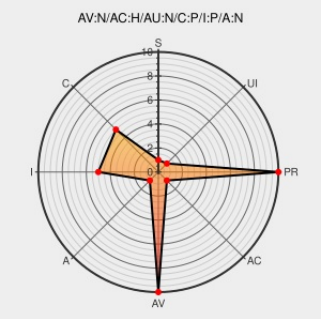
CVE-2006-4340

Published on: 09/15/2006 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:16:00 AM UTC

CVE-2006-4340

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

Mozilla Network Security Service (NSS) library before 3.11.3, as used in Mozilla Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5, when using an RSA key with exponent 3, does not properly handle extra data in a signature, which allows remote attackers to forge signatures for SSL/TLS and email certificates, a similar vulnerability to CVE-2006-4339. NOTE: on 20061107, Mozilla released an advisory stating that these versions were not completely patched by MFSA2006-60. The newer fixes for 1.5.0.7 are covered by CVE-2006-5462.

CVE-2006-4340 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Gentoo update for mozilla-thunderbird - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 22274
Sun Solaris update for Mozilla - Advisories - Secunia	web.archive.org, text/html	SECUNIA 23883
Red Hat update for thunderbird - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 21916

Avaya Products Firefox Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22422
[#RPL-640] update to firefox 1.5.0.7 and thunderbird 1.5.0.7 for critical security fixes - rPath JIRA	web.archive.org text/html Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-640
Ubuntu update for firefox - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22025
Debian update for mozilla-firefox - Advisories - Secunia	web.archive.org text/html	SECUNIA 22849
Debian -- Security Information -- DSA-1210-1 mozilla-firefox	www.debian.org Depreciated Link text/html	DEBIAN DSA-1210
Debian -- Security Information -- DSA-1192-1 mozilla	www.debian.org Depreciated Link text/html	DEBIAN DSA-1192
usn/usn-350-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-350-1
MFSA 2006-60: RSA Signature Forgery	www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/2006/mfsa2006-60.html
Mandriva update for mozilla-firefox - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22001
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22036
rPath updates for firefox and thunderbird - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21950
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:054
Gentoo update for mozilla-firefox - Advisories - Secunia	web.archive.org text/html	SECUNIA 22195
Red Hat update for firefox - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 21949
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:055
rhn.redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2006:0676
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-3899
HP-UX update for firefox - Advisories - Secunia	web.archive.org text/html	SECUNIA 22066

SecurityTracker.com Archives - Mozilla Firefox Certificate Signatures Can Be Forged	securitytracker.com text/html	SECTRACK 1016858
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2007-1198
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mozilla-nss-security-bypass(30098)
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-200609-19
Gentoo Linux Documentation -- Mozilla Network Security Service (NSS): RSA signature forgery	www.gentoo.org text/html	GENTOO GLSA-200610-06
Ubuntu update for mozilla-thunderbird - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22055
Debian update for mozilla - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22299
Debian update for mozilla-thunderbird - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22247
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11007
usn/usn-354-1 - Ubuntu: Linux for human beings	web.archive.org text/html Inactive Link Not Archived	UBUNTU USN-354-1
Mozilla Thunderbird Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21939
Bleichenbacher's RSA signature forgery based on implementation error	web.archive.org text/html Inactive Link Not Archived	MLIST [ietf-openpgp] 20060827 Bleichenbacher's RSA signature forgery based on implementation error
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060915 rPSA-2006-0169-1 firefox thunderbird
ASA-2006-224 (RHSA-2006-0675)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-224.htm
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2007-0293
Ubuntu update for mozilla-thunderbird - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22074
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2008-0083
Gentoo Linux Documentation -- Mozilla Thunderbird: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-200610-01
Debian -- Security Information -- DSA-1191-1 mozilla-thunderbird	web.archive.org text/html Inactive Link Not Archived	DEBIAN DSA-1191
SUSE update for openssl/mozilla-nss - Advisories -	web.archive.org	SECUNIA 22044

Secunia	text/html	
Ubuntu update for firefox - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22210
Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21940
Avaya CMS Sun Solaris X Display Manager Security Issue - Advisories - Secunia	web.archive.org text/html	SECUNIA 22992
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-3748
Red Hat update for seamonkey - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21915
Gentoo update for nss - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22446
SecurityTracker.com Archives - Mozilla Thunderbird Certificate Signatures Can Be Forged	securitytracker.com text/html	SECTRACK 1016860
usn/usn-352-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-352-1
Network Security Services (NSS) Signature Forgery Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21903
Netscape Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 24711
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20060901-01-P
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-3617
Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 21906
usn/usn-351-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-351-1
SUSE updates for MozillaFirefox, MozillaThunderbird, and seamonkey - Advisories - Secunia	web.archive.org text/html	SECUNIA 22056
Ubuntu update for mozilla - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22342
rhn.redhat.com | Red Hat Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2006:0675
#102648: Security Vulnerability in RSA Signature Verification Impacting Multiple SUN Products	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102648
usn/usn-361-1 - Ubuntu: Linux for human beings	www.ubuntu.com	UBUNTU USN-361-1

	text/html	
#102781: RSA Signature Forgery Issues in Mozilla 1.7 for Solaris 8, 9 and 10	web.archive.org text/html Inactive Link Not Archived	SUNALERT 102781
MFSA 2006-66: RSA Signature Forgery (variant)	www.mozilla.org text/html	MISC www.mozilla.org/security/announce/2006/mfsa2006-66.html
SecurityTracker.com Archives - Mozilla Seamonkey Certificate Signatures Can Be Forged	securitytracker.com text/html	SECTRACK 1016859
Matasano Chargen » Many RSA Signatures May Be Forgeable In OpenSSL and Elsewhere	web.archive.org text/html Inactive Link Not Archived	MISC www.matasano.com/log/469/many-rsa-signatures-may-be-forgeable-in-openssl-and-elsewhere/
rhn.redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2006:0677
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-3622
US-CERT Technical Cyber Security Alert TA06-312A -- Mozilla Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	CERT TA06-312A
IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	HP SSRT061181
ASA-2006-250 (SUN 102606, 102636, 102640, 102648, 102651, 102652, 102655, 102657)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-250.htm
Sun Solaris RSA Signature Forgery Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22226
Mandriva update for mozilla-thunderbird - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22088
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:168
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:169

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:network_security_services:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:seamonkey:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→