

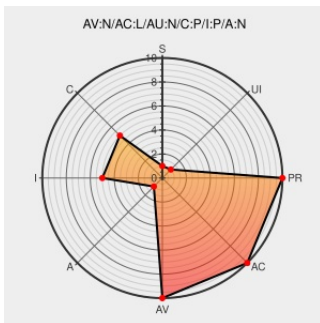


CVE-2006-5462

Published on: 11/08/2006 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:36 AM UTC

CVE-2006-5462

[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 1.5.0.8, Thunderbird before 1.5.0.8, and SeaMonkey before 1.0.6, 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. NOTE: this identifier is for unpatched product versions that were originally intended to be addressed by CVE-2006-4340.

CVE-2006-5462 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

MFSA 2006-60: RSA Signature Forgery

[Patch](#)
[www.mozilla.org
text/html](http://www.mozilla.org/text/html)

[MISC
www.mozilla.org/security/announce/2006/mfsa2006-60.html](http://www.mozilla.org/security/announce/2006/mfsa2006-60.html)

US-CERT Vulnerability Note VU#335392

[Patch](#)
[US Government Resource
www.kb.cert.org
text/html](http://www.kb.cert.org/text/html)

[CERT-VN VU#335392](http://www.kb.cert.org/text/html)

Sun Solaris update for Mozilla - Advisories - Secunia

[web.archive.org
text/html](http://web.archive.org/text/html)

[SECUNIA 23883](#)

MFSA 2006-66: RSA Signature Forgery (variant)	Patch www.mozilla.org text/html	 CONFIRM www.mozilla.org/security/announce/2006/mfsa2006-66.html
Ubuntu update for firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23009
ASA-2006-246 (RHSA-2006-0733)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-246.htm
Red Hat update for seamonkey - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22763
Debian -- Security Information -- DSA-1224-1 mozilla	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1224
rh.n.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2006:0735
Debian update for mozilla - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23197
Debian update for mozilla-firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23202
Debian update for mozilla-thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23235
Mozilla Thunderbird Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 22770
HP-UX update for firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22066
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2007-1198
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22929
Gentoo update for mozilla-firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23287
Avaya Messaging Storage Server Firefox Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22965
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF mozilla-nss-security-bypass(30098)
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10478
Mandriva update for mozilla-firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22817
SecurityTracker.com Archives - Mozilla Thunderbird RSA Signatures Can Be Forged	securitytracker.com text/html	 SECTrack 1017181
Gentoo Linux Documentation -- Mozilla Thunderbird: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200612-06
Red Hat update for firefox - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22737

SecurityTracker.com Archives - Mozilla Firefox RSA Signatures Can Be Forged	securitytracker.com text/html	 SECTrack 1017182
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2007-0293
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2008-0083
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:206
Webmail - OVH	www.vupen.com text/html	 VUPEN ADV-2006-4387
Ubuntu update for mozilla-thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23013
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2006-3748
Debian -- Security Information -- DSA-1227-1 mozilla-thunderbird	www.debian.org text/html Deprecated Link	 DEBIAN DSA-1227
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDKSA-2006:205
usn/usn-382-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	 UBUNTU USN-382-1
Debian -- Security Information -- DSA-1225-2 mozilla-firefox	www.debian.org text/html Deprecated Link	 DEBIAN DSA-1225
Gentoo Linux Documentation -- Mozilla Firefox: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200612-07
Netscape Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	 SECUNIA 24711
SecurityTracker.com Archives - Mozilla Seamonkey RSA Signatures Can Be Forged	securitytracker.com text/html	 SECTrack 1017180
Gentoo update for seamonkey - Advisories - Secunia	web.archive.org text/html	 SECUNIA 23263
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2006:068
Mandriva update for mozilla-thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22815
SUSE update for MozillaFirefox, MozillaThunderbird, and seamonkey - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22980
Red Hat update for thunderbird - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22727
356215 – FF1507 RSA signature forgery: unchecked padding length (CVE-2006-5462)	Patch bugzilla.mozilla.org text/html	 MISC bugzilla.mozilla.org/show_bug.cgi?id=356215
Gentoo Linux Documentation -- SeaMonkey: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200612-08
Mozilla Firefox and SeaMonkey Multiple	Patch	 SECUNIA 22722

Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org 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
US-CERT Technical Cyber Security Alert TA06-312A -- Mozilla Updates for Multiple Vulnerabilities	Patch 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
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20061101-01-P
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2006:0734
Gentoo update for mozilla-thunderbird - Advisories - Secunia	web.archive.org text/html	SECUNIA 23297
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2006:0733
usn/usn-381-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-381-1

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	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5	beta1	All	All
Application	Mozilla	Firefox	1.5	beta2	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	1.5.0.2	All	All	All
Application	Mozilla	Firefox	1.5.0.3	All	All	All
Application	Mozilla	Firefox	1.5.0.4	All	All	All
Application	Mozilla	Firefox	1.5.0.5	All	All	All
Application	Mozilla	Firefox	1.5.0.6	All	All	All
Application	Mozilla	Firefox	1.5.0.7	All	All	All

Application	Mozilla	Firefox	1.5	All	All	All
Application	Mozilla	Firefox	1.5	beta1	All	All
Application	Mozilla	Firefox	1.5	beta2	All	All
Application	Mozilla	Firefox	1.5.0.1	All	All	All
Application	Mozilla	Firefox	1.5.0.2	All	All	All
Application	Mozilla	Firefox	1.5.0.3	All	All	All
Application	Mozilla	Firefox	1.5.0.4	All	All	All
Application	Mozilla	Firefox	1.5.0.5	All	All	All
Application	Mozilla	Firefox	1.5.0.6	All	All	All
Application	Mozilla	Firefox	1.5.0.7	All	All	All
Application	Mozilla	Network Security Services	3.11.3	All	All	All
Application	Mozilla	Network Security Services	3.11.3	All	All	All
Application	Mozilla	Seamonkey	1.0	All	All	All
Application	Mozilla	Seamonkey	1.0	All	alpha	All
Application	Mozilla	Seamonkey	1.0	All	dev	All
Application	Mozilla	Seamonkey	1.0	beta	All	All
Application	Mozilla	Seamonkey	1.0.1	All	All	All
Application	Mozilla	Seamonkey	1.0.2	All	All	All
Application	Mozilla	Seamonkey	1.0.3	All	All	All
Application	Mozilla	Seamonkey	1.0.4	All	All	All
Application	Mozilla	Seamonkey	1.0.5	All	All	All
Application	Mozilla	Seamonkey	1.0	All	All	All
Application	Mozilla	Seamonkey	1.0	All	alpha	All
Application	Mozilla	Seamonkey	1.0	All	dev	All
Application	Mozilla	Seamonkey	1.0	beta	All	All
Application	Mozilla	Seamonkey	1.0.1	All	All	All
Application	Mozilla	Seamonkey	1.0.2	All	All	All
Application	Mozilla	Seamonkey	1.0.3	All	All	All
Application	Mozilla	Seamonkey	1.0.4	All	All	All
Application	Mozilla	Seamonkey	1.0.5	All	All	All
Application	Mozilla	Thunderbird	1.5	All	All	All
Application	Mozilla	Thunderbird	1.5	beta2	All	All
Application	Mozilla	Thunderbird	1.5.0.1	All	All	All
Application	Mozilla	Thunderbird	1.5.0.2	All	All	All
Application	Mozilla	Thunderbird	1.5.0.3	All	All	All

Application	Mozilla	Thunderbird	1.5.0.4	All	All	All
Application	Mozilla	Thunderbird	1.5.0.6	All	All	All
Application	Mozilla	Thunderbird	1.5.0.7	All	All	All
Application	Mozilla	Thunderbird	1.5	All	All	All
Application	Mozilla	Thunderbird	1.5	beta2	All	All
Application	Mozilla	Thunderbird	1.5.0.1	All	All	All
Application	Mozilla	Thunderbird	1.5.0.2	All	All	All
Application	Mozilla	Thunderbird	1.5.0.3	All	All	All
Application	Mozilla	Thunderbird	1.5.0.4	All	All	All
Application	Mozilla	Thunderbird	1.5.0.6	All	All	All
Application	Mozilla	Thunderbird	1.5.0.7	All	All	All
cpe:2.3:a:mozilla:firefox:1.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:beta2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.3:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.4:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.6:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.7:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:beta1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5:beta2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.1:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.2:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.3:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.4:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.6:*:*:*:*:*:						
cpe:2.3:a:mozilla:firefox:1.5.0.7:*:*:*:*:*:						

.....

```
cpe:2.3:a:mozilla:network_security_services:3.11.3:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:network_security_services:3.11.3:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:alpha:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:dev:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:beta:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:alpha:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:*:dev:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0:beta:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.1:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:seamonkey:1.0.5:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5:beta2:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:mozilla:thunderbird:1.5.0.7:*:*:*:*:*:*
```

cpe:2.3:a:mozilla:thunderbird:1.5:*****:
cpe:2.3:a:mozilla:thunderbird:1.5:beta2:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.1:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.2:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.3:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.4:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.6:*****:
cpe:2.3:a:mozilla:thunderbird:1.5.0.7:*****:

No vendor comments have been submitted for this CVE

← Previous IDNext ID →