# [CentOS-announce] CESA-2021:0996 Important CentOS 7 thunderbird Security Update

CentOS Errata and Security Advisory 2021:0996 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0996

The following updated files have been uploaded and are currently

syncing to the mirrors: ( sha256sum Filename )

x86_64:

412317b2522f388f60a8b9846d99020fa2c884e8557b0552ad09b4218e97803d  thunderbird-78.9.0-3.el7.centos.x86_64.rpm

Source:

9b3ff2329273f188e644f9e8fb481e12ff32397fac7f7f9b4a689aa99d84529b  thunderbird-78.9.0-3.el7.centos.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce

---

# [CentOS-announce] CESA-2021:0992 Important CentOS 7 firefox Security Update

CentOS Errata and Security Advisory 2021:0992 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0992

The following updated files have been uploaded and are currently

syncing to the mirrors: ( sha256sum Filename )

x86_64:

67cc5f25f8e6a42f9536eb9dbe7e22e3fab22c55d87d37db23cb90136913067e  firefox-78.9.0-1.el7.centos.i686.rpm

44600066daf3f3b57b9e269737e0b0dfcd410f3a524fbbd74aec3162d6f84f7c  firefox-78.9.0-1.el7.centos.x86_64.rpm

Source:

bedd47ac6fc527b008c2ed93845707f248f2a8eae9ad4201508728e2b54283

ad  firefox-78.9.0-1.el7.centos.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce

---

# USN-4893-1: Firefox vulnerabilities

Multiple security issues were discovered in Firefox. If a user were
tricked into opening a specially crafted website, an attacker could
potentially exploit these to cause a denial of service, obtain sensitive
information, or execute arbitrary code. (CVE-2021-23981, CVE-2021-23982,
CVE-2021-23983, CVE-2021-23987, CVE-2021-23988)
It was discovered that extensions could open popup windows

with control
of the window title in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to spook a website and trick the user into providing
credentials. (CVE-2021-23984)

It was discovered that the DevTools remote debugging feature could be
enabled without an indication to the user. If a local attacker could
modify the browser configuration, a remote attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23985)

It was discovered that extensions could read the response of cross
origin requests in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23986)

---

# USN-3685-2: Ruby regression

USN-3685-1 fixed a vulnerability in Ruby. The fix for CVE-2017-0903 introduced
a regression in Ruby. This update fixes the problem.
Original advisory details:

Some of these CVE were already addressed in previous
USN: 3439-1, 3553-1, 3528-1. Here we address for

the remain releases.

It was discovered that Ruby incorrectly handled certain inputs.
An attacker could use this to cause a buffer overrun. (CVE-2017-0898)

It was discovered that Ruby incorrectly handled certain files.
An attacker could use this to overwrite any file on the filesystem.
(CVE-2017-0901)

It was discovered that Ruby was vulnerable to a DNS hijacking vulnerability.
An attacker could use this to possibly force the RubyGems client to download
and install gems from a server that the attacker controls. (CVE-2017-0902)

It was discovered that Ruby incorrectly handled certain YAML files.
An attacker could use this to possibly execute arbitrary code. (CVE-2017-0903)

It was discovered that Ruby incorrectly handled certain files.
An attacker could use this to expose sensitive information.
(CVE-2017-14064)

It was discovered that Ruby incorrectly handled certain inputs.
An attacker could use this to execute arbitrary code. (CVE-2017-10784)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to inject a crafted key into a HTTP
response. (CVE-2017-17742)

It was discovered that Ruby incorrectly handled certain files. An attacker could possibly use this to execute arbitrary code. This update is only addressed to ruby2.0. (CVE-2018-1000074)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to cause a denial of service.
(CVE-2018-8777)

---

# USN-4888-2: ldb vulnerabilities

USN-4888-1 fixed several vulnerabilities in ldb. This update provides
the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly
handled certain LDAP attributes. A remote attacker could possibly use this
issue to cause the LDAP server to crash, resulting in a denial of service.
(CVE-2021-20277)

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly
handled certain DN strings. A remote attacker could use this issue to
cause the LDAP server to crash, resulting in a denial of service, or
possibly execute arbitrary code. (CVE-2020-27840)