



CVE-2019-11745

Published on: 01/08/2020 12:00:00 AM UTC

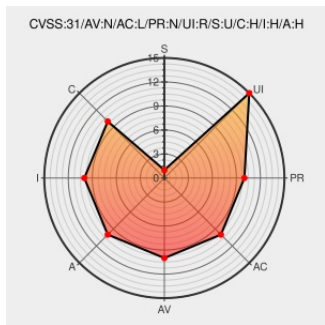
Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11745

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

When encrypting with a block cipher, if a call to NSC_EncryptUpdate was made with data smaller than the block size, a small out of bounds write could occur. This could have caused heap corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.

CVE-2019-11745 has been assigned by security@mozilla.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Mozilla - Thunderbird** version **before 68.3**

Affected Vendor/Software: **Mozilla - Firefox ESR** version **before 68.3**

Affected Vendor/Software: **Mozilla - Firefox** version **before 71**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
<p>Mozilla Thunderbird: Multiple vulnerabilities (GLSA 202003-10) — Gentoo security</p>	<p>Third Party Advisory security.gentoo.org text/html</p>	<p><input type="checkbox"/> GENTOO GLSA-202003-10</p>
<p>Mozilla Network Security Service: Multiple vulnerabilities (GLSA 202003-37) — Gentoo security</p>	<p>Third Party Advisory security.gentoo.org text/html</p>	<p><input type="checkbox"/> GENTOO GLSA-202003-37</p>
<p>Mozilla Firefox: Multiple vulnerabilities (GLSA 202003-02) — Gentoo security</p>	<p>Third Party Advisory security.gentoo.org text/html</p>	<p><input type="checkbox"/> GENTOO GLSA-202003-02</p>
<p>Red Hat Customer Portal</p>	<p>Third Party Advisory access.redhat.com text/html</p>	<p><input type="checkbox"/> REDHAT RHSA-2020:0243</p>
<p>Security Vulnerabilities fixed in - Firefox 71 — Mozilla</p>	<p>Vendor Advisory www.mozilla.org text/html</p>	<p><input type="checkbox"/> CONFIRM www.mozilla.org/security/advisories/mfsa2019-36/</p>
<p>Siemens RUGGEDCOM ROX II CISA</p>	<p>Third Party Advisory US Government Resource us-cert.cisa.gov text/html</p>	<p><input type="checkbox"/> MISC us-cert.cisa.gov/ics/advisories/icsa-21-040-04</p>
<p>Red Hat Customer Portal</p>	<p>Third Party Advisory access.redhat.com text/html</p>	<p><input type="checkbox"/> REDHAT RHSA-2020:0466</p>
<p>Security Vulnerabilities fixed in - Thunderbird 68.3 — Mozilla</p>	<p>Vendor Advisory web.archive.org text/html Inactive Link Not Archived</p>	<p><input type="checkbox"/> CONFIRM www.mozilla.org/security/advisories/mfsa2019-38/</p>
<p>[security-announce] openSUSE-SU-2020:0003-1: important: Security update</p>	<p>Mailing List Third Party Advisory lists.opensuse.org text/html</p>	<p><input type="checkbox"/> SUSE openSUSE-SU-2020:0003</p>
<p>[security-announce] openSUSE-SU-2020:0002-1: important: Security update</p>	<p>Issue Tracking Mailing List Third Party Advisory lists.opensuse.org text/html</p>	<p><input type="checkbox"/> SUSE openSUSE-SU-2020:0002</p>
<p>USN-4335-1: Thunderbird vulnerabilities Ubuntu security notices</p>	<p>Third Party Advisory usn.ubuntu.com text/html</p>	<p><input type="checkbox"/> UBUNTU USN-4335-1</p>
<p>Security Vulnerabilities fixed in - Firefox ESR 68.3 — Mozilla</p>	<p>Vendor Advisory www.mozilla.org text/html</p>	<p><input type="checkbox"/> CONFIRM www.mozilla.org/security/advisories/mfsa2019-37/</p>
<p>[SECURITY] [DLA 2388-1] nss security update</p>	<p>Mailing List Third Party Advisory lists.debian.org text/html</p>	<p><input type="checkbox"/> MLIST [debian-lts-announce] 20200929 [SECURITY] [DLA 2388-1] nss security update</p>
<p>1586176 - (CVE-2019-11745) Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate</p>	<p>Issue Tracking Patch Vendor Advisory bugzilla.mozilla.org text/html</p>	<p><input type="checkbox"/> CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=1586176</p>

[Third Party Advisory](#)
[cert-portal.siemens.com](#)
[application/pdf](#)

CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-379803.pdf

[security-announce] openSUSE-SU-2020:0008-1: moderate: Security update f

[Mailing List](#)
[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

SUSE openSUSE-SU-2020:0008

USN-4241-1: Thunderbird vulnerabilities | Ubuntu security notices | Ubuntu

[Third Party Advisory](#)
[usn.ubuntu.com](#)
[text/html](#)

UBUNTU USN-4241-1

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.

Related QID Numbers

[256751](#) CentOS Security Update for nss (CESA-2019:4190)

[500455](#) Alpine Linux Security Update for nss

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

System						
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Hardware	Siemens	Ruggedcom Rox Mx5000	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Mx5000	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Mx5000 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Mx5000 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1400	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1400	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1400 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1400 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1500	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1500	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1500 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1500 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1501	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1501	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1501 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1501 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1510	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1510	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1510 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1510 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1511	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1511	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1511 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1511 Firmware	All	All	All	All

System						
Hardware	Siemens	Ruggedcom Rox Rx1512	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx1512	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1512 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx1512 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx5000	-	All	All	All
Hardware	Siemens	Ruggedcom Rox Rx5000	-	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx5000 Firmware	All	All	All	All
Operating System	Siemens	Ruggedcom Rox Rx5000 Firmware	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:~:~:~:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:~:~:~:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:~:~:~:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:~:~:~:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:~:~:~:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:~:~:~:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:~:~:~:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:~:~:~:						
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:~:~:~:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:~:~:~:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:~:~:~:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:~:~:~:						
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:*:*:*:*:*:~:~:~:						
cpe:2.3:h:siemens:ruggedcom_rox_mx5000:-:*:*:*:*:*:~:~:~:						
cpe:2.3:h:siemens:ruggedcom_rox_mx5000:-:*:*:*:*:*:~:~:~:						

cpe:2.3:o:siemens:ruggedcom_rox_mx5000_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_mx5000_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1400:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1400:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1400_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1400_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1500:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1500:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1500_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1500_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1501:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1501:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1501_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1501_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1510:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1510:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1510_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1510_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1511:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1511:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1511_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1511_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1512:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx1512:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1512_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx1512_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx5000:-:*:*:*:*:*:

cpe:2.3:h:siemens:ruggedcom_rox_rx5000:-:*:*:*:*:*:

cpe:2.3:o:siemens:ruggedcom_rox_rx5000_firmware:*.:.:.:.:.:.:.:.:.:.:

cpe:2.3:o:siemens:ruggedcom_rox_rx5000_firmware:*.:.:.:.:.:.:.:.:.:.:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)