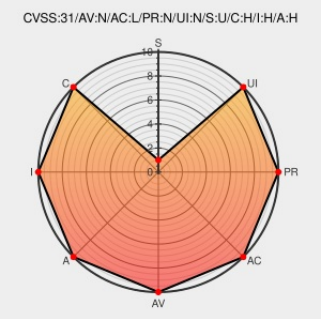
CVE-2019-18609

Published on: 12/01/2019 12:00:00 AM UTC

Last Modified on: 01/01/2022 08:06:00 PM UTC

CVE-2019-18609

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

An issue was discovered in amqp_handle_input in amqp_connection.c in rabbitmq-c 0.9.0. There is an integer overflow that leads to heap memory corruption in the handling of CONNECTION_STATE_HEADER. A rogue server could return a malicious frame header that leads to a smaller target_size value than needed. This condition is then carried on to a memcpy function that copies too much data into a heap buffer.

CVE-2019-18609 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 31 Update: librabbitmq-0.10.0	Third Party Advisory	FEDORA-FEDORA-2019-8720b65158

[SECURITY] Fedora 31 Update: librabbitmq-0.10.0-1.fc31 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2019-8730b65158
RabbitMQ integer overflow that leads to heap memory corruption | Hacker News	Issue Tracking Third Party Advisory news.ycombinator.com text/html	MISC news.ycombinator.com/item?id=21681976
[SECURITY] [DLA 2022-1] librabbitmq security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20191206 [SECURITY] [DLA 2022-1] librabbitmq security update
lib: check frame_size is >= INT32_MAX · alanxz/rabbitmq-c@fc85be7 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/alanxz/rabbitmq-c/commit/fc85be7123050b91b054e45b91c78d3241a5047a
USN-4214-1: RabbitMQ vulnerability | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4214-1
[SECURITY] Fedora 30 Update: librabbitmq-0.10.0-1.fc30 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2019-dd7c8f5435
USN-4214-2: RabbitMQ vulnerability | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4214-2
RabbitMQ C client: Arbitrary code execution (GLSA 202003-07) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-07
rabbitmq-c/ChangeLog.md at master · alanxz/rabbitmq-c · GitHub	Third Party Advisory github.com text/html	MISC github.com/alanxz/rabbitmq-c/blob/master/ChangeLog.md

Related QID Numbers

377376 Alibaba Cloud Linux Security Update for librabbitmq (ALINUX3-SA-2022:0078)

377528 Alibaba Cloud Linux Security Update for librabbitmq (ALINUX2-SA-2020:0136)

690097 Free Berkeley Software Distribution (FreeBSD) Security Update for rabbitmq-c (7c555ce3-658d-4589-83dd-4b6a31c5d610)

940137 AlmaLinux Security Update for librabbitmq (ALSA-2020:4445)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Rabbitmq-c Project	Rabbitmq-c	All	All	All	All
Application	Rabbitmq-c Project	Rabbitmq-c	0.9.0	All	All	All
Application	Rabbitmq-c Project	Rabbitmq-c	0.9.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:a:rabbitmq-c_project:rabbitmq-c:*:*:*:*:*:*:*:*:

cpe:2.3:a:rabbitmq-c_project:rabbitmq-c:0.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:rabbitmq-c_project:rabbitmq-c:0.9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→