



CVE-2019-9193

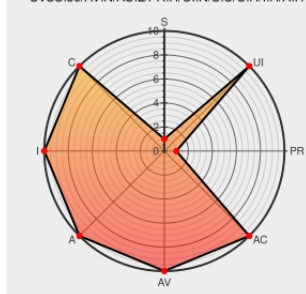
Published on: 04/01/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:13:00 AM UTC

CVE-2019-9193

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Postgresql](#) from [Postgresql](#) contain the following vulnerability:

**** DISPUTED **** In PostgreSQL 9.3 through 11.2, the "COPY TO/FROM PROGRAM" function allows superusers and users in the 'pg_execute_server_program' group to execute arbitrary code in the context of the database's operating system user. This functionality is enabled by default and can be abused to run arbitrary operating

system commands on Windows, Linux, and macOS. NOTE: Third parties claim/state this is not an issue because PostgreSQL functionality for 'COPY TO/FROM PROGRAM' is acting as intended. References state that in PostgreSQL, a superuser can execute commands as the server user without using the 'COPY FROM PROGRAM'.

CVE-2019-9193 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Internet Archive: Scheduled Maintenance	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/166540/PostgreSQL-11.7-Remote-Code-Execution.html
Authenticated Arbitrary Command Execution on PostgreSQL 9.3 > Latest Trustwave	Third Party Advisory www.trustwave.com text/html	 MISC www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/authenticated-arbitrary-command-execution-on-postgresql-9-3/
Postgres 9.3 feature highlight - COPY TO/FROM PROGRAM	Third Party Advisory paquier.xyz text/html	 MISC paquier.xyz/postgresql-2/postgres-9-3-feature-highlight-copy-tofrom-program/
When a vulnerability is not a vulnerability - Magnus Hagander's blog	Third Party Advisory blog.hagander.net text/html	 MISC blog.hagander.net/when-a-vulnerability-is-not-a-vulnerability-244/
PostgreSQL COPY FROM PROGRAM Command Execution ≈ Packet Storm	Third Party Advisory packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/152757/PostgreSQL-COPY-FROM-PROGRAM-Command-Execution.html
Authenticated Arbitrary Command Execution on PostgreSQL 9.3 > Latest	Exploit Third Party Advisory medium.com text/html	 MISC medium.com/greenwolf-security/authenticated-arbitrary-command-execution-on-postgresql-9-3-latest-cd18945914d5
PostgreSQL 9.6.1 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/171722/PostgreSQL-9.6.1-Remote-Code-Execution.html
CVE-2019-9193 PostgreSQL in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190502-0003/

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

Exploit/POC from Github

PostgreSQL Remote Code Executuon

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	All	All	All	All

cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

 @twittersupport	(2) ,cve-2015-4642,cve-2009-4143,cve-2019-0708,cve-2019-9193,cve-2007-1581,cve-2011-4109,cve-2008-5557,cve-2004-049... twitter.com/i/web/status/1...	2021-05-12 03:59:51
 @johnk3r	This shell is part of the post-exploration of CVE-2019-9193. The objective is to do bitcoin mining. The observed... twitter.com/i/web/status/1...	2021-07-21 22:56:50
 @GuillermoVersus	Si una prestación puede ser insegura o no según su uso ¿se convierte en vulnerabilidad? security-tracker.debian.org/tracker/CVE-20...	2021-11-13 08:31:36
 @grambulf	@JGamblin How do you feel about this one? (If I may ask) postgresql.org/about/news/cve... blog.hagander.net/when-a-vulnera...	2021-12-08 14:59:41
 @grambulf	@JGamblin I agree with you. As far as I remember some said that the Postgres CVE-2019-9193 should never have been a... twitter.com/i/web/status/1...	2021-12-08 15:44:47

[< Previous ID](#)
[Next ID >](#)

© CVE.report 2023   |

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report