



CVE-2019-16662

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-16662
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-28 12:15:00 UTC
Updated	2019-10-29 19:15:00 UTC
Description	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rconfig	Rconfig	3.9.2	All	All	All
Application	Rconfig	Rconfig	3.9.2	All	All	All

References

Reference	Source	Link
rConfig-preauth.png - Google Drive	MISC	drive.goo
rConfig v3.9.2 authenticated and unauthenticated RCE (CVE-2019-16663) and (CVE-2019-16662) - Shells.Systems	MISC	shells.sys
rConfig 3.9.2 Command Injection ≈ Packet Storm	MISC	packetsto
rConfig -Network Configuration Management	MISC	rconfig.co
rConfig 3.9.2 Remote Code Execution ≈ Packet Storm	MISC	packetsto
The script exploits a preauth RCE in rConfig v3.9.2 · GitHub	MISC	gist.githu
rConfig-preauth.mp4 - Google Drive	MISC	drive.goo
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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