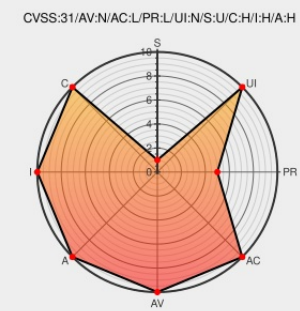
CVE-2019-16663

Published on: 10/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16663

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



Certain versions of Rconfig from Rconfig contain the following vulnerability:

An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to search.crud.php because the catCommand parameter is passed to the exec function without filtering, which can lead to command execution.

CVE-2019-16663 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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
rConfig v3.9.2 authenticated and unauthenticated RCE (CVE-2019-16663) and (CVE-2019-16662) - Shells.Systems	Exploit Technical Description Third Party Advisory shells.systems text/html	MISC shells.systems/rconfig-v3-9-2-authenticated-and-unauthenticated-rce-cve-2019-16663-and-cve-2019-16662/

The script exploits a postauth RCE in rConfig v3.9.2 Raw · GitHub	Exploit Third Party Advisory gist.github.com text/html	MISC gist.github.com/mhaskar/e7e454c7cb0dd9a139b0a43691e258a0
rConfig -Network Configuration Management	Product rconfig.com text/html	MISC rconfig.com/download
rConfig-postauth.png - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/open?id=1kQGmboKfwob4RwlMjnv6ER2Za1GUptOi
rConfig-PostAuth-2019-09-20_11.39.23.mp4 - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/open?id=1XmR2MSMb3cKARFk3XxmPkwz6GhAP1JxL

There are currently no QIDs associated with this CVE

Exploit/POC from Github

The official exploit for rConfig 3.9.2 Post-auth Remote Code Execution CVE-2019-16663

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:rconfig:rconfig:3.9.2:*:*:*:*:*:*:*

cpe:2.3:a:rconfig:rconfig:3.9.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2019-16663.… twitter.com/i/web/status/1…	2021-04-26 07:02:00
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2019-16663. ipssignatures.appspot.com/?cve=CVE-2019-… #Srpn53qewxfnj6	2021-04-26 07:02:01
@ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2019-16663.… twitter.com/i/web/status/1…	2021-07-27 01:02:00

@ipssignatures	twitter.com/i/web/status/1…	01:02:00
@ipssignatures	I know 4 other IPSs that have protections/signatures/rules for the vulnerability CVE-2019-16663. ipssignatures.appspot.com/?cve=CVE-2019-… #Srpn53qewxfnj6	2021-07-27 01:02:00

← Previous ID

Next ID→