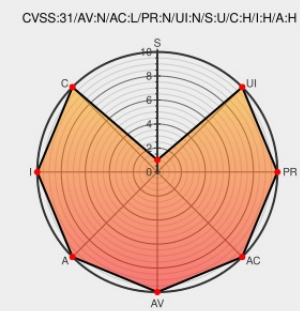
CVE-2022-36231

Published on: Not Yet Published

Last Modified on: 03/03/2023 07:28:00 PM UTC

CVE-2022-36231

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



Certain versions of Pdf Info from Newspaperclub contain the following vulnerability:

pdf_info 0.5.3 is vulnerable to Command Execution because the Ruby code uses backticks instead of Open3.

CVE-2022-36231 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

CVE References

Description	Tags	Link
Fix CVE command injection by tomtaylor · Pull Request #15 · newspaperclub/pdf_info · GitHub	github.com text/html	MISC github.com/newspaperclub/pdf_info/pull/15
GitHub - affix/CVE-2022-36231: pdf_info <= 0.5.3 OS Command Injection	github.com text/html	MISC github.com/affix/CVE-2022-36231
pdf_info | RubyGems.org | your community gem host	rubygems.org text/html	MISC rubygems.org/gems/pdf_info
"command execution" vulnerability, CVE-2022-36231 · Issue #16 · newspaperclub/pdf_info · GitHub	github.com text/html	MISC github.com/newspaperclub/pdf_info/issues/16

There are currently no QIDs associated with this CVE

Exploit/POC from Github

pdf_info <= 0.5.3 OS Command Injection

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Newspaperclub	Pdf Info	0.5.3	All	All	All

cpe:2.3:a:newspaperclub:pdf_info:0.5.3:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@deepquest	ruby gem pdf_info <= 0.5.3 is vulnerable to OS Command Injection when executing a method on a PDF::Info object. github.com/affix/CVE-2022…	2022-10-27 07:00:04
@hack_git	CVE-2022-36231 The ruby gem pdf_info <= 0.5.3 is vulnerable to OS Command Injection when executing a method on a P… twitter.com/i/web/status/1…	2022-10-28 09:10:31
@CVEreport	CVE-2022-36231 : pdf_info 0.5.3 is vulnerable to Command Execution.... cve.report/CVE-2022-36231	2023-02-23 22:07:40
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-36231 pdf_info 0.5.3 is vulnerable to Command Execution.... CVSS: 9.21 #CVE #CyberSecurity	2023-02-23 22:56:00
/r/netcve	CVE-2022-36231	2023-02-23 22:38:31

← Previous ID

Next ID→