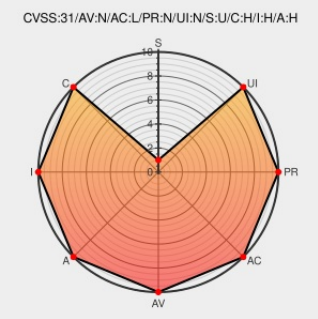
CVE-2018-1000533

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 09/09/2021 05:36:00 PM UTC

CVE-2018-1000533

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



Certain versions of Gitlist from Gitlist contain the following vulnerability:

klaussilveira GitList version <= 0.6 contains a Passing incorrectly sanitized input to system function vulnerability in `searchTree` function that can result in Execute any code as PHP user. This attack appear to be exploitable via Send POST request using search form. This vulnerability appears to have been fixed in 0.7 after commit 87b8c26b023c3fc37f0796b14bb13710f397b322.

CVE-2018-1000533 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
Fixed RCE in git grep. · klaussilveira/gitlist@87b8c26 · GitHub	Patch Third Party Advisory github.com	MISC github.com/klaussilveira/gitlist/commit/87b8c26b023c3fc37f0796b14bb13710f3

	text/html	
Exploit/bypass PHP escapeshellarg/escapeshellcmd functions · security.szurek.pl	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC security.szurek.pl/exploit-bypass-php-escapeshellarg-escapeshellcmd

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

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:gitlist:gitlist:*:*:*:*:*:*:*:*:

cpe:2.3:a:gitlist:gitlist:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→