



CVE-2014-4511

Published on: 07/22/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4511

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

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

Gitlist before 0.5.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the file name in the URI of a request for a (1) blame, (2) file, or (3) stats page, as demonstrated by requests to blame/master/, master/, and stats/master/.

CVE-2014-4511 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

gitlist - commit to rce - forelsec

[Exploit](#)
[hatriot.github.io](#)
[text/html](#)

[MISC hatriot.github.io/blog/2014/06/29/gitlist-rce/](#)

Google Groups

[groups.google.com](#)
[text/html](#)

CONFIRM
[groups.google.com/forum/#!topic/gitlist/Hw_KdZfA4js](#)

Gitlist Unauthenticated Remote Command Execution

[Exploit](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

EXPLOIT-DB 33990

Gitlist 0.4.0 Remote Code Execution ≈ Packet Storm

[Exploit](#)
[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/127281/Gitlist-0.4.0-Remote-Code-Execution.html](#)

Gitlist Unauthenticated Remote Command

[Exploit](#)

MISC [packetstormsecurity.com/files/127364/Gitlist-](#)

Gitlist <= 0.4.0 - Remote Code Execution

Exploit
www.exploit-db.com
Proof of Concept
text/html

EXPLOIT-DB 33929

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

CVE-2014-4511

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlist	Gitlist	0.1	All	All	All
Application	Gitlist	Gitlist	0.2	All	All	All
Application	Gitlist	Gitlist	0.3	All	All	All
Application	Gitlist	Gitlist	All	All	All	All
Application	Gitlist	Gitlist	0.1	All	All	All
Application	Gitlist	Gitlist	0.2	All	All	All
Application	Gitlist	Gitlist	0.3	All	All	All
cpe:2.3:a:gitlist:gitlist:0.1:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:0.2:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:0.3:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:0.1:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:0.2:*:*:*:*:*:						
cpe:2.3:a:gitlist:gitlist:0.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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