



CVE-2021-37364

Published on: 10/26/2021 12:00:00 AM UTC

Last Modified on: 10/28/2021 10:01:00 PM UTC

CVE-2021-37364

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

Certain versions of [Openclinic Ga](#) from [Openclinic Ga Project](#) contain the following vulnerability:

OpenClinic GA 5.194.18 is affected by Insecure Permissions. By default the Authenticated Users group has the modify permission to openclinic folders/files. A low privilege account is able to rename mysqld.exe or tomcat8.exe files located in bin folders and replace with a malicious file that would connect back to an attacking computer

giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.

CVE-2021-37364 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link				
OpenClinic GA 5.194.18 - Local Privilege Escalation - Windows local Exploit	www.exploit-db.com Proof of Concept text/html	 MISC www.exploit-db.com/exploits/50448				
OpenClinic GA download SourceForge.net	sourceforge.net text/html	 MISC sourceforge.net/projects/open-clinic/				
Download OpenClinic GA from SourceForge.net	sourceforge.net text/html	 MISC sourceforge.net/projects/open-clinic/files/latest/download				
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	Openclinic Ga Project	Openclinic Ga	5.194.18	All	All	All
cpe:2.3:a:openclinic_ga_project:openclinic_ga:5.194.18:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2021-37364 : OpenClinic GA 5.194.18 is affected by Insecure Permissions. By default the Authenticated Users gro... twitter.com/i/web/status/1...					2021-10-26 14:09:24

[← Previous ID](#)

[Next ID →](#)