Talos Vulnerability Report

TALOS-2020-1204

OpenClinic GA installation privilege escalation vulnerability

APRIL 13, 2021

CVE NUMBER

CVE-2020-27228

Summary

An incorrect default permissions vulnerability exists in the installation functionality of OpenClinic GA 5.173.3. Overwriting the binary can result in privilege escalation. An attacker can replace a file to exploit this vulnerability.

Tested Versions

OpenClinic GA 5.173.3

Product URLs

https://sourceforge.net/projects/open-clinic/

CVSSv3 Score

8.8 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

OpenClinic GA is an open source fully integrated hospital management solution.

OpenClinic GA 5.173.3 is installed in “C:\projects\openclinic" directory (it currently does not allow installation in another directory) and it allows “Authenticated Users” to have change privilege over “OpenClinicMySQL” service binary file in the directory which are executed with NT SYSTEM authority. This allows users of any authenticated group to read, write or modify arbitrary files in the install directory resulting in privilege escalation when service is restarted.

```
c:\projects\openclinic\mysql5\bin\mysqld.exe

BUILTIN\Administrators:(ID)F
NT AUTHORITY\SYSTEM:(ID)F
BUILTIN\Users:(ID)R
NT AUTHORITY\Authenticated Users:(ID)C
```

Timeline

2020-11-19 - Initial contact
2020-12-07 - 2nd contact; copy of advisories issued and vendor acknowledged receipt
2021-02-01 - 60 day follow up; no response
2021-03-09 - 90 day follow up; no response
2021-03-22 - Final notice

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1205

NEXT REPORT TALOS-2020-1203