HC3: Sector Alert
January 31, 2023 TLP:CLEAR Report: 202301311200

Multiple Vulnerabilities in OpenEMR Electronic Health Records System

Executive Summary
Three vulnerabilities were identified in an older version of OpenEMR, a popular electronic health records system, which can allow for a cyberattacker to access sensitive information and even compromise the entire system. The prevalence of ransomware attacks and data breaches impacting the health sector make these vulnerabilities especially important. These vulnerabilities were fixed in newer versions of OpeEMR, and therefore upgrading to the most recent version will fully patch them.

Report
The software development solution company, Sonar, released a report identifying three vulnerbilities in an older version of OpenEMR, a popular electronic health records system. OpenEMR is described as being "used by more than 100,000 medical providers serving more than 200 million patients". The three vulnerabilities are Unauthenticated File Read, Authenticated Local File Inclusion, and Authenticated Reflected XSS. These vulnerabilities all represent opportunities for cybercriminals to launch ransomware attacks and data breaches – both of which are persistent threats to the health sector, among other types of attacks.

Vulnerabilities
Technical details of the vulnerabilities can be found in the Sonar alert. This includes the attack lifecycle for all three vulnerabilities. It also details how an attacker-controlled MySQL configuration can lead to exploitation of the arbitrary file read vulnerability and how combining two code vulnerabilities, Cross-Site Scripting, and Local File Inclusion can lead to a takeover of any OpenEMR instance. These vulnerabilities were initially reported by Sonar to OpenEMR on October 24, 2022 and released in version 7.0.0, which included the three patches, on November 30, 2022.

Patches, Mitigations, and Workarounds
OpenEMR released version 7.0.0 with patches on November 30, 2022. The link to these updates can be found here. In order to fully prevent these vulnerabilities from exploitation, older versions of the software should be updated immediately.

References
OpenEMR - Remote Code Execution in your Healthcare System
https://www.sonarsource.com/blog/openemr-remote-code-execution-in-your-healthcare-system/

OpenEMR Patches: 7.0.0 Patch (11/30/22)
https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#7.0.0_Patch_.2811.2F30.2F22.29

Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback