OpenEMR Flaw Potentially Exposes Medical Records
Date: 05/25/2018

Healthcare Cybersecurity and Communications Integration Center (HCCIC) HHSHCCIC@HHS.GOV

SUMMARY

OpenEMR is a free, open-source electronic health records and medical practice management application that was found to have a vulnerability that could lead to the disclosure, corruption, or loss of access to patient medical records and other patient data. OpenEMR features include patient scheduling, billing, prescriptions, and medical records management functions. OpenEMR is used at more than 5,000 physician offices and other small healthcare facilities that serve an estimated 30 million patients in the United States.[i] Although this vulnerability was originally disclosed in November of 2017, some installations remain unpatched and at least one pen-testing company has recently advertised the ability to take advantage of the vulnerability.

DISCUSSION

The disclosed OpenEMR vulnerability occurs in earlier versions of the software (before 5.0.0 patch 6) which fail to delete a critical setup file after installation; leaving it accessible to attackers. With this vulnerability, an attacker could copy the entire contents of the OpenEMR database, modify patient or practice information, or even deny access to appropriate users. The information accessible to an attacker through this vulnerability is likely to include sensitive information such as passwords and protected health information (PHI).[ii] As of November 2017, 141 of 188 (or 75%) of the publicly visible installations of OpenEMR remained susceptible to the vulnerability.[ii] Available information suggests that a large number of the organizations may still be at risk. For more technical details on mitigating the risk of the vulnerability in OpenEMR, see below.

Organizations and their supporting IT providers within the Healthcare and Public Health Sector (HPH) that use OpenEMR are advised to take a few steps to mitigate the risk of unauthorized data access or loss of use:

- Verify they are using the latest version of the OpenEMR application.
- Upgrade to the most recent version of OpenEMR.
- If it is not possible to upgrade to newer versions of the software, or if the organization is working with a cloud service provider, the administrator should manually remove the setup.php file from the OpenEMR installation.

TECHNICAL INFORMATION ABOUT THE EXPLOIT

In OpenEMR versions before v.5.0.0 patch 6, a vulnerability (CVE-2017-16540) exists in which the "setup.php" script remains after installing OpenEMR. Unauthenticated remote attackers can exploit the setup.php script in multiple ways. Access to the setup script could grant an attacker the ability to copy the entire site—including protected health information (PHI)—to an attacker-controlled MySQL server via vectors involving a crafted state parameter.[iii] This new attacker-controlled site will then have access to the original database, allowing the attacker to gain administrative access to the original OpenEMR installation.[ii] With this administrative access the attacker has the potential to edit local PHP files, insert arbitrary PHP code, disclose patient data, or install malicious software, such as ransomware.

TECHNICAL MITIGATION

Organizations and their supporting IT providers within the HPH that use OpenEMR are advised to take a few steps to mitigate the risk of unauthorized data access or loss of use. Organizations should work with providers to patch on premise and cloud hosted instances of OpenEMR. All organizations are encouraged to test and deploy one of the following fixes to mitigate the risk of unauthorized access to medical records from this vulnerability:

- If using OpenEMR version 5.0.0, upgrade to version 5.0.1 patch 2 which was released on May 7, 2018[iv]
- If using OpenEMR version 4.2.2 or lower:
  - Upgrade to version 5.0.1 patch 2[v]
  - If it is impossible to upgrade to 5.0.1 patch 2, manually remove the setup.php file from the site.[vi]
- Additionally, if using cloud instances such as Amazon, Microsoft, and Google:
  - Manually remove the setup.php file and consult your provider on patching.

Before installing any OpenEMR patches, administrators should check the list of files that the OpenEMR patch will overwrite and save backup copies of any customized files (List of Files).[vii]

For administrators concerned that attackers may be attempting (or have attempted) to exploit this vulnerability, check apache error logs for the following entry:

```
mysqldump: [Warning] Using a password on the command line interface can be insecure.
```

Although this warning will also occur during a legitimate OpenEMR migration, it's definitely not something that should happen during typical operation. The appearance of this warning in the error log outside of a planned site migration is a fairly good indication that the database has been compromised using techniques outlined in this article.[viii]

This report was prepared by the Healthcare Cybersecurity and Communications Integration Center (HCCIC). This is an analysis of vulnerabilities that continue to be researched and analyzed. Readers are advised to search for the latest authoritative information and exercise professional judgment before taking actions related to any vulnerability.

REFERENCES

[i] "OpenEMR Security Vulnerability Could Expose Medical Records Impacting 90M Patients," December 20, 2017 accessed January 16, 2018; http://hitconsultant.net/2017/12/20/openemr-flaw-which-could-expose-medical-records/

[ii] Zelijka Zorz, "OpenEMR flaw leaves millions of medical records exposed to attackers", 29 November 2017, accessed 3 January 2018; https://www.helpnetsecurity.com/2017/11/29/openemr-flaw-medical-records-exposed/

[iii] NIST, "CVE-2017-16540" published November 4 2017 accessed January 16, 2018 https://nvd.nist.gov/vuln/detail/CVE-2017-16540
[iv] OpenEMR Patches; http://www.open-emr.org/wiki/index.php/OpenEMR_Patches
[v] OpenEMR Upgrade Guidelines; http://www.open-emr.org/wiki/index.php/OpenEMR_Wiki_Home_Page
[vi] OpenEMR, "Critical Security Fix for Open EMR setup.php" accessed January 16, 2018; http://www.open-emr.org/wiki/index.php/Critical_Security_Fix_for_OpenEMR_setup.php
[vii] OpenEMR Patches List of Files, https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#List_of_files_.285.0.1.29
[viii] "OpenEMR: CVE-2017-16540," Undocumented APIs, 28 October 2017, accessed 22 May 2018; https://isears.github.io/jekyll/update/2017/10/28/openemr-database-disclosure.html