RBS-2017-001

OpenEMR Multisite Setup Improper Access Restriction Remote Code Execution

Vendor / Product Information

OpenEMR is a Free and Open Source electronic health records and medical practice management application. It is ONC Certified and features e.g. fully integrated electronic health records, practice management, scheduling, electronic billing, internationalization, and free support. It can run on Windows, Linux, Mac OS X, and many other platforms.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	OpenEMR Project
Product:	OpenEMR
Component:	setup.php
Version:	5.0.0

NOTE: Other versions than the one listed above are likely affected.

Credits

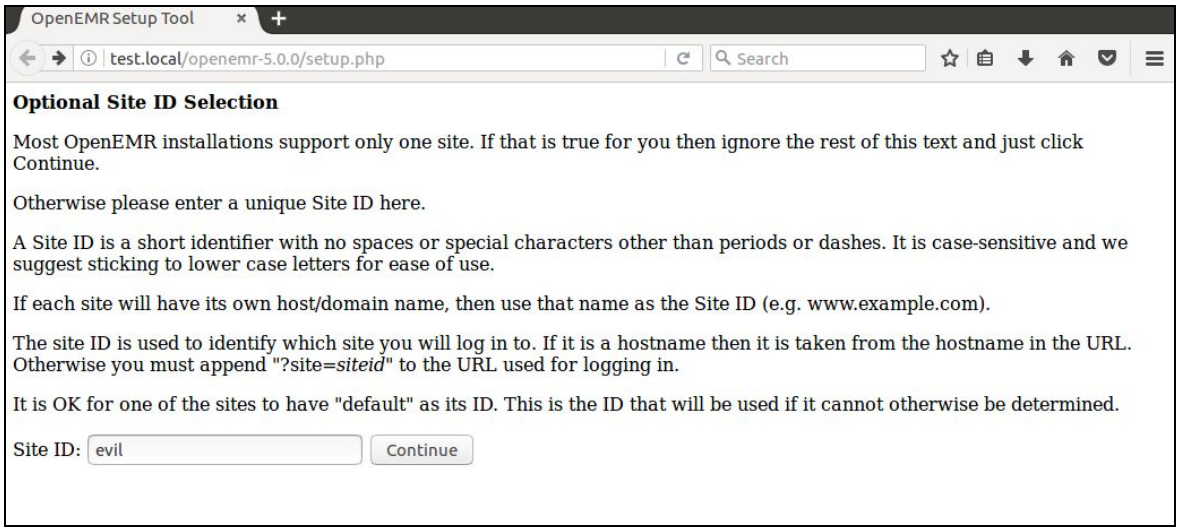
Sven Krewitt, Risk Based Security
Twitter: @RiskBased

Impact

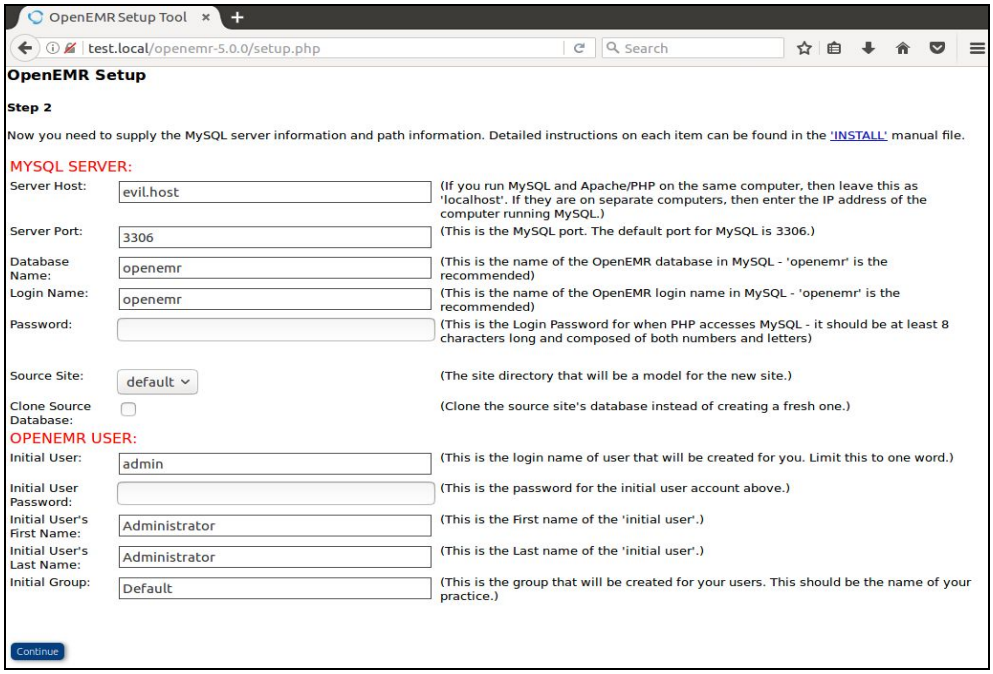
OpenEMR contains a `setup.php` file that is used during the web-based installation of the application. Although the documentation vaguely recommends to remove the file after the installation routine is finished, it fails to warn about the risks of keeping the file. It was discovered that certain functionality can be accessed if the file remains in the web directory that may allow a remote attacker to gain administrative access to the application and execute arbitrary PHP code.

Vulnerability Details

When accessing setup.php after an initial installation, the script responds with a notification about an Optional Site ID Selection. Providing a site ID that is not already configured, the script then continues the an installation routine for an additional site (multi-site).



This allows a remote attacker to enter arbitrary database configuration parameters. Besides exploiting previously reported SQL injection vulnerabilities, this allows configuring a multi-site setup with an attacker-controlled MySQL database and configuring the administrator credentials.



After finishing the setup routine, a remote attacker can access the OpenEMR application using the site ID and the provided credentials. The attacker now has administrator privileges for the newly configured site.

Using the `Administration->Files` menu, it is further possible to edit local PHP files and subsequently execute arbitrary PHP code in context of the web server. The application suggests that there is a separation of sensitive patient data between different sites, but sensitive uploaded files are stored in the directory structure and can be accessed with web server privileges.

Solution

The vendor has issued OpenEMR 5.0.0 Patch 6 (5.0.0.6).

References

RBS:	RBS-2017-001[1]
VulnDB:	156368

Timeline

2017-11-07	Vulnerability reported to the OpenEMR Project
2017-11-07	Vendor acknowledged vulnerability
2017-11-17	Vendor publishes security patch
2018-02-01	Alert sent to RBS VulnDB clients
2018-03-22	Publication of this vulnerability report.

[1] https://www.riskbasedsecurity.com/research/RBS-2017-001.pdf

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.