Managing Security Vulnerabilities in OpenMRS

OpenMRS seeks to be a reliable and trusted application. We also recognize that security incidents can (and do) still happen, and so it's just as important to have effective methods for handling them should they arise.

A Security Group currently exists on OpenMRS Talk. Membership is by invitation only and is open to existing members of the OpenMRS community working on security issues.

Anyone can send in reports via email to security@openmrs.org.

A framework for managing security incidents

To ensure our incident response process is consistent, repeatable and efficient, we have a clearly defined internal framework that covers the steps we need to take at each phase of the incident response process.

Receipt of Incident

Community members and concerned parties work with OpenMRS' Security Group in logging, monitoring of our artifacts and infrastructure to ensure we quickly detect potential incident

The designated mechanism through which security incidents are reported is via email on **security@openmrs.org.** Details of the incident are shared on the Security Talk category for discussion.

Assessment of Incident :

The Security Group will review the incident report and determine an incident severity categorization as depicted below:

Severity Level	Characteristic	Time to resolve (Days)
Critical	• The exploitation of the vulnerability likely results in a root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions. For critical vulnerabilities, it is advised that you patch or upgrade as soon as possible unless you have other mitigating measures in place. For example, a mitigating factor could be if your installation is not accessible from the Internet.	90
High	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in significant data loss or downtime.	180
Medium	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.	180
Low	Vulnerabilities in the low range typically have *very little impact* on an organization's business. The exploitation of such vulnerabilities usually requires local or physical system access.	1 Year

Routine security updates will be highlighted in the release notes for each release. If a vulnerability is a critical one (e.g something submitted by an external body), members will receive an email to that effect

Containment, eradication, and recovery

The security vulnerabilities group will determine depending on the level of severity of the incident, agree what corrective measures need to be taken to cont ain the incident, eradicate the underlying causes and start our recovery processes to ensure that operations return to normal. Thus a summary of activities at this stage would include:

1. Upon receipt of incident the security vulnerabilities group is activated: Identify an “Owner,” developer, others on the core team
2. Minimum a team of 3-5 people can be assigned to a certain vulnerability group i-e ‘Owner’, ‘developer’ and a ‘tester’,'coordinator' etc.

3. The team can be formed by a security management team with discussion to OpenMRS management, based upon previous contributions of members in their concerned (security) area.
4. Define a plan of action to be agreed and executed upon
5. We also have access to a range of external experts to assist us with investigating and responding as effectively as possible.
6. Work on the fix
7. Compliance with the deadlines
8. Test and release
9. Create an initial draft of the security review and circulate for review
10. Deploy to our environments
11. Notify the public via OpenMRS Talk
12. Vulnerability with its solution and updated fixes be documented properly. (if possible within major other languages also.)

Notification :

We aim to notify affected community members within 5 business days or without undue delay if their data is involved in an incident or a breach. This might be light on detail at first, but we'll provide every detail available when it is available. These initial communications will be done directly with the affected party as the matter is being resolved, however, as soon as the security group deems that it is possible to inform a broader audience, such information will be posted to the designated communication channel which is OpenMRS Talk.

Notification Format:

Security Advisory Format

Contains at a minimum:

- Severity
- Exploit
- Affected versions (including mentioning EOL'd versions)
- Exact steps on how to fix the problem, and any available workarounds (list exact versions)
- Acknowledgments to people who reported it and fixed it.

Security Group

Role:

The role of the group is to work with the finder or reporter to resolve the identified vulnerability. It is also tasked to continually review and understand vulnerabilities that are currently occurring within the system either by themselves or via programs such as bug bounties. This group is responsible for identifying the requisite resources needed to address any vulnerabilities addressed.

Scope of activities:

1. Identify requisite resources to develop fixes for identified vulnerabilities
2. Oversee at least one major vulnerability scan a year and map a corrective action plan to address vulnerabilities identified

Roles within the Security Group:

- **Finder (Discoverer/ Reporter)** – the individual or organization that identifies the vulnerability
    - External group (i.e: Bishop Fox)
    - Internally (i.e:bug bounty/Hackerone)
- **Manager** - An individual with a role of managing the vulnerability process till the fixing and its updated release, appointed by the management of OpenMRS.
- **Vendor** – the individual or organization that created or maintains the vulnerable product.
- **Deployer –** the individual or organization that must deploy a patch or take other remediation action
    - Implementers
    - Release managers who need to include the patch in the ongoing release process
- **Coordinator –** an individual or organization that facilitates the coordinated response process
    - TPM
    - OpenMRS Software Security Lead
- **Tester** -the individual who tests the updated release, its feedback is taken from the Deployer and documents the fixes finally report it to the "Owner".

Security Vulnerability "Manager" - Roles and Responsibilities

1. Deciding (with the core team) which versions should be released
2. Ensuring that a developer is working on the problem on a timely fashion
3. Ensuring that a release is done as soon as possible
4. Create the initial draft of the security advisory and ask for reviews. Create the CVE if relevant.
5. Follow the process to release the security advisory
6. Ensure all public OpenMRS community environments are updated.
7. Follow up on any discussions or questions about the incident.
8. Ensuring the documentation of vulnerabilities and their updated solutions to have a review for the next developments.
9. Ensuring the proper testing of the Vulnerability fixing by cross-checking by with the pre-vulnerability state and documenting the final report for future use.