Errata - 1.6 Security Update, March 2015

Summary

This vulnerability affects all installations of Open-AudIT prior to version 1.6.2.

A patched version of Open-AudIT (1.6.2) is available from http://www.open-audit.org/downloads.php and https://opmantek.com/network-tools-download/.

Users are advised to upgrade ASAP.

Details

A vulnerability affecting the web view files is caused because of insufficient output escaping. The vulnerability requires an Admin level user to purposely insert javascript into a field that can be displayed in the web pages. This issue has been addressed by a review of all web view files in Open-AudIT to ensure all output is sufficiently escaped before being sent to the browser.

Severity: Medium

The conditions of successful exploitation are that the attacker must have Admin level access to Open-AudIT and maliciously insert javascript code to a field that is (was) not correctly escaped prior to browser output.

Products Affected

Open-AudIT 1.6 for Windows and earlier. Open-AudIT Enterprise is not affected by this vulnerability.

Available Updates

A patch for the issue described in this bulletin is available in the newly released Open-AudIT v1.6.2. This release is available now on http://www.openaudit.org and https://opmantek.com.

Workarounds and Mitigations

Upgrade to Open-AudIT 1.6.2

The vulnerability was addressed by Opmantek and upgrading to Open-AudIT 1.6.2 will include this fix and remove the vulnerability.

The preferred method of mitigation is an upgrade to Open-AudIT 1.6.2.

Customers can further mitigate this threat by proactively changing the default passwords as shipped with Open-AudIT.