Errata - 2.1 Security Update, April 2018

Summary

This issue affects all installations of Open-AudIT prior to version 2.2.

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

Users are advised to upgrade ASAP to Open-AudIT 2.2.

This issue was reported to us by Suresh Narvaneni (thanks Suresh). A link the the CVE is https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9137

Details

If a user deliberately injects characters into a field that is exported to CSV and opens the CSV with Microsoft Excel and ignores the warning that Excel will execute the data contained in the CSV, the user can inject any Windows command.

The issue has been addressed by including a new configuration item called output_escape_csv which is set to 'y' by default. If a value contains =, +, -, @ as its first character, a single quote is inserted.

Severity: Low

The conditions of successful exploitation are that the attacker must have a role with the ability to edit items in Open-AudIT and maliciously insert =, +, -, @ as the first character of a field along with the malicious command(s). The target must then download data containing that field and ignore the warning when opening it with MS Excel that the data will be executed (as opposed to simply viewed).

Products Affected

Open-AudIT 2.1 and earlier.

Available Updates

A patch for the issue described in this bulletin is available in the Open-AudIT v2.2 release. This release is available from http://www.openaudit.org and https://opmantek.com.

Workarounds and Mitigations

Upgrade to Open-AudIT 2.2.

The issue was addressed by Opmantek and upgrading to Open-AudIT 2.2 will include this fix and remove the issue.

The preferred method of mitigation is an upgrade to Open-AudIT 2.2.