Errata - 1.5.3 Security Update, February 2015

Summary

This only affects Windows installations of Open-AudIT. This DOES NOT affect Linux installations of Open-AudIT.

A patched version of Open-AudIT (1.5.4) 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 all Windows perl code that uses File::Spec has been discovered that allows an attacker to download local files in some conditions. Part of the Open-AudIT program uses a framework known as Mojolicious which in turn uses this perl module. This issue is confirmed to affect all Windows Open-AudIT installations prior to v1.5.4. Users on platforms others than windows are not affected. The vulnerability has been addressed by the Mojolicious framework upgrade to 5.76 as detailed on this page https://metacpan.org/release/SRI/Mojolicious-5.76.

Severity: Medium

The conditions of successful exploitation are that the attacker must know that OpenAudIT use this framework and that the exploiter has access to the Open-AudIT Server. Individual files from the Open-AudIT server's C: drive can be downloaded if the correct (and full) paths are known.

Products Affected

Open-AudIT 1.5.3 for Windows and earlier.

Note: This only impacts the Open-AudIT server for Windows, this vulnerability does not affect devices that are audited.

Available Updates

A patch for the issue described in this bulletin is available in the newly released Open-AudIT v1.5.4 for Windows. This release is available now on http://www.openaudit.org and https://opmantek.com.

Workarounds and Mitigations

Upgrade to Open-AudIT 1.5.4

The vulnerability was addressed by the publishers of the Mojolicious framework and upgrading to Open-AudIT 1.5.4 will include this fix and remove the vulnerability. If customers cannot do this they can stop the "omkd" service from running under Windows Services, but this will prevent Open-AudIT from fully functioning.

The preferred method of mitigation is an upgrade to 1.5.4 for Windows.