Errata - 3.1.2 Security issue, September 2019

Summary

This issue affects all installations of Open-AudIT prior to version 3.2.0.

A new 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 3.2.0.

This issue was reported to us by Jack Cable (thanks Jack). A link the the CVE is https://nvd.nist.gov/vuln/detail/CVE-2019-16293

Details

If an authenticated user with Discovery Create permissions deliberately injects characters into the field that contains the URL on the Create Discoveries template, the field contents will be passed to the command line that runs the discovery script and be executed. The user can inject any command.

The issue has been addressed by filtering any characters for this input that are not:

```
a-z
A-Z
0-9
/
:
```

This filtering occurs both at time of submission and upon command creation.

Severity: Low

The conditions of successful exploitation are that the attacker must have a role with the ability to edit discoveries in Open-AudIT and maliciously insert characters to break the command execution.

Products Affected

Open-AudIT 3.1.2 and earlier.

Available Updates

A patch for the issue described in this bulletin is available in the Open-AudIT v3.2.0 release. This release is available from http://www.openaudit.org and https://opmantek.com.

Workarounds and Mitigations

Upgrade to Open-AudIT 3.2.0.

The issue was addressed by Opmantek and upgrading to Open-AudIT 3.2.0 will include this fix and remove the issue.

The preferred method of mitigation is an upgrade to Open-AudIT 3.2.0.