Recently reported vulnerabilities within Open-AudIT

Some of you may have read about some recently reported vulnerabilities within Open-AudIT. This post seeks to explain and clarify these, along with detailing further fixes implemented.

The vulnerabilities fall into one of two categories - cross site scripting and code execution.

For the record, I ***do*** consider these to be vulnerabilities, however I find them to be quite contrived. In all cases you must be logged into Open-AudIT (no unauthenticated issues have been found) and in the case of the code execution bugs, you have to also be an Admin in Open-AudIT. For me personally, I consider that if you're an Admin you can already see the device credentials and could therefore run any code you like using a shell anyway. As said - I ***do*** consider these as vulnerabilities, but not earth shattering. Actually more concerning is the XSS vulnerability (of the two). A logged in Open-AudIT user could craft a link and send it to a more privileged Open-AudIT user, who opens it and can have arbitrary JavaScript run in their browser. *Maybe* a privilege escalation issue could occur in the application. If you have users who you do not trust that are using Open-AudIT, I think you have bigger problems. Again, **yes** it is a vulnerability. I just consider it minimal in the grand scheme of things.

So what are we doing to address these? Well obviously we have released new code that addresses all the reported issues. If you do not wish to upgrade and are a supported customer, Opmantek will also provide assistance regarding patching your existing install. Really though - just upgrade. We have made other improvements besides these fixes and it is well worth your time.

What have we done in addition to this? We have been through user input and sanitized it against known types, for a start. IE - If you change the configuration log_level value, it must be an integer. Previously we did do some validation, but it turns out not enough (for contrived issues). Another example is the user supplied SQL for groups, queries and widgets. From now on, we reject any SQL that contains INSERT, UPDATE or DELETE clauses (and variations there-of). Again - if you're letting a user create queries you should be trusting them to do so in the first place. But we have tightened this up regardless. For other items such as attributes, files and scripts we have also now restricted what we accept in various fields. These restrictions may possibly affect the odd user, but should not be overly restrictive and no existing entries will be changed. We also found some minor cross site scripting issues (un-sanitized output) in some standard templates. We have now escaped these and as a result they may look ugly, but they are safe. And if you manage to see one of these, looking pretty is not what I am concerned with, I'm more interested in "why are you seeing ***that***".

So there it is - nothing major (in my opinion) but I feel if you are forewarned, you are armed.

As always, please upgrade to the latest available release for these fixes along with many other new improvements.

The Release Notes pages detail what changes for each release and I would encourage you to read them every time we release.

If you have any questions or concerns, feel free to reach out to us here at Opmantek. I recommend the Questions site so everyone else can also see your question and our response.

Mark Unwin.