TARANIS

Vulnerability Management

Taranis 3.4

Release Notes

TARANIS

Vulnerability Management

TARANIS

Vulnerability Management

Taranis 3.4

Release Notes

National Cyber Security Centre

Turfmarkt 147 | 2511 DP The Hague

PO box 117 | 2501 CC The Hague

T +31 70 751 55 55 | F +31 70 888 75 50

www.ncsc.nl | info@ncsc.nl

Index

1 New features and enhancements

Taranis version 3.4 is the successor of version 3.3. It contains about one and a half year of development and maintenance effort. This document gives a brief overview on the changes made.

The CHANGES file in the distribution list a few more, like some of the fixed bugs. This document's focus is on the global overview.

1.1 Automated installation

The installation procedure of Taranis has been reworked. In previous releases, the administrator had to go through to a large number of manual actions to get Taranis running, but in the new release this has been automated. Most of the work to get this running is answering a few questions.

The installation now creates a dedicated username to run the application. All used files get a place under the home directory of this user. Also, the cron-jobs will be run with the permission of this username. This even works for upgrading the software. That implies that the administrator of Taranis does not need root rights anymore, once a first version has been installed.

1.2 Perl modules from CPAN

In previous releases, Taranis used Perl packages as distributed by the Linux distribution where it got installed. From now on, close to all Perl modules are installed in their latest version, directly from CPAN – Perl's Open Source software archief. This brings the newest features and bugfixes.

As a disadvantage, it takes some time during the first installation run to install these modules, even on a fast internet connection.

1.3 Structure of an instance

With the new installation structure, you can install different versions of Taranis in parallel. This means that you can upgrade and role-back between minor updates without hassle. Read the release-notes carefully, because database changes may not be revertible; there shouldn't be many conflicts between minor upgrades.

You may even install an incompatible major upgrade under a different username on the same server, without conflict. This is especially useful in a testing environment: run the upcoming release, but still have access to a working copy of the production version.

Previous versions of Taranis mixed its own code with user data. The user data and configuration define an instance. The components of an installation are cleanly separated now: a clean separation between:

- raw release data: ~taranis/sources/taranis-3.4.0/
- the installed version of Taranis: ~taranis/taranis-3.4.0/
- your local generic extensions: ~taranis/local/
- your local, version specific extensions: ~taranis/local-3.4.0/
- configurable instance data: ~taranis/etc/
- generated configuration: ~taranis/lib/
- instance data in files: ~taranis/var/
- instance data in the database: postgresql database 'taranis'

At first upgrade, scripts will try to reorganize your existing 3.3 installation into the new structure. it will update your taranis.conf.xml file to match the new set-up. However, this process may not be perfect.

1.4 Documentation

Most of the pages in the installation and migration documents became superfluous with this new installation procedure. The migration manual has therefore been merged as small chapter into the installation document.

1.5 Environment

Taranis 3.4 installation is only supported on the CentOS7 and Ubuntu 16.04LTS. Newer releases may work. OpenSUSE and RedHat may work for you as well.

2 Maintenance

2.1 Manual intervention from the command-line

Many administrative tasks of Taranis can be executed via the graphical interface. However, a few dozen tasks were run from the command-line or via crontab. Mainly, the 'collector' process triggered a lot of (un)related activities. This has changed: the large task has been fragmented into many small tasks.

The "collector.pl" and many loose admin and back-end scripts have all been rewritten into more than 30 separate sub-commands of a new "taranis" command. You can run these sub-commands by hand, when you need debugging or have some urgency. When required, the scripts lock themselves to avoid two instances to be run at the same time. Also, each command has a separate logfile in a standard format.

2.2 Automatic maintenance

A large number of the new sub-commands of the "taranis" command have to be run on specific intervals. Where they formed a part of "collector.pl" in the previous release, they now form a part of scripts named ~taranis/var/cron.* They are located between other files which define your instance: you are free to modify these files. Each script contains a list of maintenance steps which are executed in order.

3 Improvements on existing features

3.1 Improvements

- Twitter feeds will not index retweets anymore.
- The same sources and assess items may appear in different categories, to be handled by different (groups of) people.
- Text searches are much faster: we require a recent PostgreSQL version, which supports trigram indexes.
- Passwords are now hashed with bcrypt, improving on the SHA512 of previous releases. The hash of the password in the database will automatically be upgraded when a user logs in.
- Many string length restrictions in database have been removed.
- Emails were build with Mail::Builder, now with Mail::Message which produces a better result.
- Advisory emails which have a TLP:Amber text, with have the text "TLP:AMBER" prepended to the subject of the messages.
- Archiving of items is considerably faster.
- By default, the list of hardware and software to select for the creation of an advisory is limited to the ones which are actually being used by your constituents.

4 New features

- Taranis now has a logo. There now is a clean way to add your own logo.
- Work has been done towards "late links" for new "End-Of-Day White" messages. This is part of changing procedures within NCSC, and currently disabled by default.
- A new icon will copy the text of an item to the clipboard, in a practical paste-able layout.