

The OISF development team is proud to announce Suricata 1.2beta1. This is the first beta release for the upcoming 1.2 version. It brings major new features.

This release has been the result of very rapid development the last month, as can be seen in the change stats:

234 files changed, 24250 insertions(+), 6813 deletions(-)

As a result of these significant changes the release is expected to be of beta quality.

Get the new release here: <http://www.openinfosecfoundation.org/download/suricata-1.2beta1.tar.gz>

Compilation of this code requires the magic library and development files. The library is usually already installed, the development files are usually not. On Debian/Ubuntu install libmagic-dev, on Fedora file-devel.

New features

- File name, type inspection and extraction for HTTP
- filename, fileext, filemagic and filestore keywords added
- "file" output for storing extracted files to disk
- file_data keyword support, inspecting normalized, dechunked, decompressed HTTP response body (feature #241)
- new keyword http_server_body, pcre regex /S option
- Option to enable/disable core dumping from the suricata.yaml (enabled by default)
- Human readable size limit settings in suricata.yaml (bug #333)
- PF_RING bpf support (required PF_RING >= 5.1) (feature #334)
- tos keyword support (feature #364)
- IPFW IPS mode does now support multiple divert sockets
- New IPS running modes, Linux and FreeBSD do now support "worker" and "autofp"

Improvements

- improved alert accuracy in autofp and single runmodes
- major performance optimizations for the ac-gfbs pattern matcher implementation
- unified2 output fixes
- PF_RING supports privilege dropping now (bug #367)
- Improved detection of duplicate signatures

- Improved performance in virtual machines (bug #382)

Known issues & missing features

In a beta release like this things may not be as polished yet. So please handle with care. That said, if you encounter issues, please let us know! As always, we are doing our best to make you aware of continuing development and items within the engine that are not yet complete or optimal. With this in mind, please notice the list we have included of known items we are working on.

See <http://redmine.openinfosecfoundation.org/projects/suricata/issues> for an up to date list and to report new issues. See http://redmine.openinfosecfoundation.org/projects/suricata/wiki/Known_issues for a discussion and time line for the major issues.