Wednesday, January 12, 2022

ClamAV 0.103.5 and 0.104.2 security patch release; 0.102 past EOL

ClamAV versions 0.103.5 and 0.104.2 are now available for download on the clamav.net Downloads page.

We would also like to take this opportunity to remind users that versions 0.102 and 0.101 have reached their end-of-life period. These versions exceeded our EOL dates on Jan. 3, 2022 and will soon be actively blocked from downloading signature database updates.

For additional details about ClamAV's end-of-life policy, please see our online documentation.

0.103.5

ClamAV 0.103.5 is a critical patch release with the following fixes:

- CVE-2022-20698: Fix for invalid pointer read that may cause a crash. This issue affects 0.104.1, 0.103.4 and prior when ClamAV is compiled with libjson-c and the `CL_SCAN_GENERAL_COLLECT_METADATA` scan option (the `clamscan --gen-json` option) is enabled.

  Cisco would like to thank Laurent Delosieres of ManoMano for reporting this vulnerability.

- Fixed ability to disable the file size limit with libclamav C API, like this:

  ```
  cl_engine_set_num(engine, CL_ENGINE_MAX_FILESIZE, 0);
  ```

  This issue didn't affect ClamD or ClamScan which also can disable the limit by setting it to zero using `MaxFileSize 0` in `clamd.conf` for ClamD, or `clamscan --max-filesize=0` for ClamScan.

  Note: Internally, the max file size is still set to 2 GiB. Disabling the limit for a scan will fall back on the internal 2 GiB limitation.

- Increased the maximum line length for ClamAV config files from 512 bytes to 1,024 bytes to allow for longer config option strings.

- SigTool: Fix insufficient buffer size for `--list-sigs` that caused a failure when listing a database containing one or more very long signatures. This fix was backported from 0.104.

Special thanks to the following for code contributions and bug reports:

- Laurent Delosieres

0.104.2

ClamAV 0.104.2 is a critical patch release with the following fixes:

- **CVE-2022-20698**: Fix for invalid pointer read that may cause a crash. Affects 0.104.1, 0.103.4 and prior when ClamAV is compiled with libjson-c and the `CL_SCAN_GENERAL_COLLECT_METADATA` scan option (the `clamscan --gen-json` option) is enabled.

  Cisco would like to thank Laurent Delosieres of ManoMano for reporting this vulnerability.

- Fixed ability to disable the file size limit with libclamav C API, like this:

  ```
  cl_engine_set_num(engine, CL_ENGINE_MAX_FILESIZE, 0);
  ```

  This issue didn't impact ClamD or ClamScan which also can disable the limit by setting it to zero using `MaxFileSize 0` in `clamd.conf` for ClamD, or `clamscan --max-filesize=0` for ClamScan.

  Note: Internally, the max file size is still set to 2 GiB. Disabling the limit for a scan will fall back on the internal 2 GiB limitation.

- Increased the maximum line length for ClamAV config files from 512 bytes to 1,024 bytes to allow for longer config option strings.

Special thanks to the following for code contributions and bug reports:

- Laurent Delosieres

Posted by Micah Snyder at 2:11 PM

Labels: 0.103.5, 0.104.2, clamav, eol

Contributors

Alain Zidouemba

Angel M. Villegas

Christine Council

Dave Raynor

Jon Munshaw

Katherine Hill

MTaylor

Matthew Watchinski

Micah Snyder

Mickey Sola

Nick Herbert

Prasanth Bondalapati

Twillowkins