Release Note GCap 2.5.3.104

Gatewatcher

Created on : Janvier, 2021

Last updated : April, 2021

Table of contents

Chapter 1

Release Note GCap 2.5.3.104

You will find:

- Patches.
- Known issues.

Chapter 2

Patches

2.1 Correction of the workload distribution of Suricata

Some CPUs were not used to their full potential. This bug was caused by the LXC containerisation technology taking it upon itself to perform an unexpected and unwanted system corruption. This tampering was removed from the LXC code, and balancing was restored.

2.2 Corruption of legitimate flow detection

Suricata 4.1.6 contained a vendor patch related to CVE-2019-18625 to prevent certain detection bypass techniques.

Due to this patch, some legitimate streams were not detected.

We have disabled this patch to restore proper detection of these streams.

Versions 2.5.3.101 and earlier were not affected by this bug.

2.3 Fixed a problem recognising some .zip file formats

Since version v2.5.3.102, a bug had been introduced for the detection of certain .zip files. This was related to excessive performance optimisation. This fix allows all .zip files to be detected correctly, without sacrificing performance.

2.4 File extraction problem during some TCP transactions

All versions of Suricata (4.X, 5.X, and 6.X) have a bug that erroneously reports that an extracted file of interest has not been extracted. The problem appears for TCP sessions running as follows:

- Initial handshake.
- PUSH of a file in its entirety without any ACK.
- ACK of all segments and closing the connection by RST.

This erroneous report disrupts the operation of the GCap which does not send the file to the GCenter.

While waiting for an official patch, we have compensated for this problem by developing a partial patch that still sends the files to the GCenter which does not disturb the operation of the GCap. However, this patch cannot retrieve the metadata associated with the files affected by this bug. The metadata reported for these files are therefore wrong, we have set them to recognizable values:

127.0.0.1 for the source and destination IP address. * **12345** for the source and destination TCP port. * Transport protocol **http**.

The added patch is triggered periodically every 15 minutes and therefore introduces a latency between the time the files are retrieved from the GCap and the time they are sent to the GCenter.

2.5 Fixed a stability issue with the rule update daemon

The daemon in charge of updating the rules could stop unexpectedly when connectivity to the GCenter was lost. This error had a very low probability of occurring and was present since version 2.5.3.2. The patch ensures that the condition under which the error occurs is better controlled so that it no longer causes the unexpected shutdown, and logs the event.

2.6 Fixed generation of file rebuild rules when using interface clusters in multi-tenant mode

When interface clusters were used, in combination with the use of multi-tenant detection rulesets, a problem could arise in the generation of file reconstruction rules. the generation of rules related to file reconstruction. This could render file rebuilding inoperative in this case.

Chapter 3

Known problems

3.1 TCP transactions and extracted files

All versions of Suricata (4.X, 5.X, and 6.X) have a bug that erroneously reports that an extracted file of interest has not been extracted. The problem appears for TCP sessions running as follows:

- Initial handshake.
- PUSH of a file in its entirety without any ACK.
- ACK of all segments and closing the connection by RST.

This erroneous report disrupts the operation of the GCap which does not send the file to the GCenter.

A partial fix is present in versions greater than or equal to 2.5.3.104.

3.2 Resetting the GCap

The reset function is not reliable enough in GCap versions equal to or higher than 2.5.3.103, and has been disabled. Its operation will be reviewed and corrected in its entirety in version 2.5.3.105.

3.3 Erroneous status display of the monitoring interfaces

When the network card fails, the status of the affected interface displayed by the configuration utility may be incorrect.

3.4 Replay of PCAP files

The “replay pcap” function is not operational when multi-tenancy per interface is used.

3.5 Protection of the authentication mechanism (anti-bruteforce)

The authentication attempt counter is incremented whenever a login attempt is made, even if no password is entered by the user.