Release Note GCap 2.5.3.103

Gatewatcher

Created on : Janvier, 2021

Last updated : April, 2021

Table of contents

Chapter 1

Release Note GCap 2.5.3.103

You will find:

- New features.
- Patches.
- Known issues.

Chapter 2

New features

2.1 Aggregating the monitoring interfaces

The system for aggregating monitoring interfaces (interface clusters) was revised to improve its reliability. It is now possible to connect a GCap to a broadband TAP dividing the upstream and downstream flows. A cluster is made up of exactly two monitoring interfaces. These clusters can be configured by means of the GCap configuration interfaces.

2.2 Detection rules per monitoring interface and per VLAN (multi-tenancy)

Support for separate detection rule sets was added. These rulesets may be applied to monitoring interfaces or to specific VLANs. This configuration is performed from a compatible GCenter (see GCenter release notes). For the time being, support for per-interface detection rules is limited in combination with interface clusters.

2.3 Detection engine

The start-up and shutdown procedure of the detection engine was revised in order to improve controls on the integrity of its components. At every start-up, it checks the connectivity of the monitoring interfaces linked to the GCap. It must have at least one active interface or cluster to launch. It also ensures that the filtering rules are applied on the relevant monitoring interfaces. The detection engine logs were consolidated for simplicity. The strengthening of the detection engine was carried out, creating an environment with more constrained resources and more restrictive permissions.

2.4 Command Line Interface (CLI)

It is now possible to modify the GCap configuration via a command line interface (CLI). The CLI is now the default GCap configuration interface for all users. Each user can decide to reset the graphical user interface as their default interface. This interface will adapt to the current state of the GCap and the user's privileges. This aims to present the user with only relevant commands. Configuring local detection rules as well as packet filtering (XDP) is only possible through the graphical interface.

2.5 User account and password

As of GCap version 2.5.3.103, it is possible to change user passwords at any time, even if the detection engine is running. This modification enables forcing the change of passwords upon the first connection. This also enabled adding the notion of a maximum life span in the password policy. In addition, a maximum connection duration for a session was added. After this time limit, the session is automatically closed. This duration is configurable and optional. A warning is included regarding the use of the 'root' account that invalidates the support.

2.6 Criticality levels of application logs

The consistency of application log criticality levels was improved.

2.7 Pre-authentication SSH banner

A banner displayed before the SSH authentication can be configured on compatible GCenters.

2.8 Text editor for the input of local detection rules

The interface for entering local detection rules was improved. It is now performed in a more advanced text editor.

2.9 System strengthening

Protection against program corruption is now provided as soon as the GCap is started.

2.10 Protocol and logging management

The detection engine is now capable of analysing new protocols: — Kerberos — DHCP — TFTP — IKEv2 — NFS — NTP By default, all these new protocols are analysed and their metadata is logged. The management of selected protocols such as FTP, DNS, and SMB was also improved. For security reasons, reconstructing the SMB and FTP flows was limited to 10MB. DNS eve-log management was improved.

2.11 New compatibility mode with the GCenter

UA new compatibility mode named "GCenter v101+" was added to the GCap. With this mode, it is possible to delegate the configuration of the new protocols (see Protocol and logging management) to GCenter versions 2.5.3.101 or higher. In the other possible compatibility modes, the activation/deactivation of these new protocols is made through the GCap configuration interfaces.

2.12 Replaying flow in PCAP format

It is possible to replay a flow in PCAP format. This enables emulating network traffic, in order to perform functional tests of the probe. This feature can only be activated when used in combination with a compatible GCenter.

2.13 Improved system logging

The system logs were expanded to include information regarding the success and failure of file transfers to the GCenter.

2.14 Bruteforce protection

Protection against SSH password bruteforce was added to the GCap. It is possible to configure the number of attempts and the lockout time.

2.15 Pre-filtering of eve-logs

Fileinfo events for files not saved for later analysis can now be deleted by GCap. This prevents the GCenter from being overloaded with potentially unnecessary information. This pre-filtering can be enabled or disabled.

2.16 Log compression

It is now possible to compress logs pending submission to the GCenter. It is advisable to enable this feature in situations of intermittent connectivity, or any other problem that prevents logs from being sent to the GCenter. It is disabled by default for performance considerations.

2.17 Reducing the attack surface on the GCap

The software component securing container applications was replaced by a lighter and more configurable application. This enables reducing the attack surface and refining the security checks performed on the containers.

2.18 GCap 1000 series

Version 2.5.3.103 supports the GCaps 1000 series.

Chapter 3

Patches

3.1 Updating the detection engine

The detection engine was updated to integrate the patches from the open-source solution's editor.

3.2 Updating the container system

A number of sensitive applications that make up the GCap are placed in system containers. These were updated to include the latest security patches.

3.3 Reconfiguring the detection engine

During the detection engine's reconfiguration, too much information was being logged. More actions are hence being logged and the information is more consistent.

3.4 Refreshing the interface status

The refresh button in the "Interfaces" menu now correctly updates the status of interfaces.

3.5 Setting up the password policy

It was possible to configure a password policy with values that were either negative or far too large. Minimum and maximum values were established.

3.6 Correcting the start and stop conditions of services

When restarting a GCap after a power failure, some services refused to launch, as they were being detected as already running. The management of temporary files was corrected to avoid this situation during unexpected restarts. The start sequence of the detection engine was also incorrect. Following a start-up involving an error, the engine would start up automatically when the error was resolved, instead of on demand.

3.7 RESET function

The 'reset' function was deleted.

3.8 Strengthening the network routing configuration

The network configuration was automatically modified by a system service. This modification weakened the strengthened routing rules that were established. The previous status did not have a significant impact because if flows were routed due to the lax configuration, they were stopped by the firewall. The system service responsible for the lax configuration was replaced by a less intrusive version. Routing is now properly strengthened.

3.9 'Unexpected' error message

When the detection engine would stop, the logs recorded an inaccurate error message. The message indicated an "unexpected and exceptional" error whereas it was in fact "expected and tolerable".

3.10 Stopping the synchronisation service

A sudden stoppage of the synchronisation service of the rules and configuration files between a GCap and the GCenter was possible. The problem was caused by multiple simultaneous attempts to delete the same temporary file. The deletion process was improved. Unexpected stoppages could also occur during connectivity problems or if files caused an error in the file type inference library. In addition, the service could sometimes take too long to stop, especially during network configuration changes. The service was optimised to shorten this timeframe.

3.11 Sending extracted files

The grace period before extracted files can no longer be transferred between a GCap and a GCenter was extended. This change enables improved compatibility with connectivity-limited networks.

3.12 Network interface names

Generating network interface names could be incorrect due to exceptional cases such as connecting SPFs not recognised by the kernel's network drivers. The management was redesigned to correct this problem.

3.13 Generating fileinfo type events

Fileinfo type events were always generated, even if file extraction was disabled. Traffic generation was inconsistent with the requested configuration.

3.14 Netdata logs

It is possible to view the netdata logs from the "inspect" menu.

3.15 Extracting by file extension

The extensions to be extracted, defined from the GCenter web interface, are now extracted by the GCap.

Chapter 4

Known problems

4.1 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.

4.2 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.

4.3 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.

4.4 Replay of PCAP files

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

4.5 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.