Revision C

McAfee Web Gateway 9.0.x Release Notes

Contents

What's new in the 9.0 release

Releases can introduce new features and enhancements or update platform support.

McAfee® Web Gateway 9.0 is provided as a controlled release. For upgrade information, see the *McAfee Web Gateway Installation Guide*.

Support for Azure Key Vault as HSM technology for Hybrid

Azure Key Vault is the only cloud HSM that is 100% API based and does not require installing a client or agent. As such it is best suited for cloud-to-cloud key security.

Transparent Bridge mode resumed

Web Gateway can be run as a proxy in Transparent Bridge mode again. This network mode had temporarily not been available due a change in the product architecture.

File opening scope enlarged

The scope of the Open XML file opener has been enlarged. This opener now makes custom properties data available for DLP inspection in addition to the document data that is already extracted.

New options for configuring network communication

Several new options have been implemented to enhance network protocol handling on Web Gateway.

- Priority can be configured for WCCP services.
- Uptime and DHCP IP addresses are displayed on the user interface.
- gRCP trailing headers are supported under HTTP2.

No FIPS certification

The product is no longer certified to comply with FIPS regulations. Web Gateway 7.8.2 is the latest product version that is FIPS-certified.

Resolved issues in update 9.0.1

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.0.1 is provided as a controlled release. For upgrade information, see the *McAfee Web Gateway Installation Guide*.

Hyper-V 2019 support

All Web Gateway product versions now support use of a Windows 2019 server in a Hyper-V role.

Transparent Bridge mode resumed

Web Gateway can be run as a proxy in Transparent Bridge mode again. This network mode had temporarily not been available due a change in the product architecture.

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference columns of the tables below.

Table 2-1 Network communication

Reference	Resolution
WP-1843	The user interface no longer disappears intermittently when Web Gateway is running as a High Availability proxy.
WP-2049	The X-Forwarded-For Header is filled with the value for the IP address of the client that sent a particular request when Web Gateway is running as a High Availability proxy, whereas the field had previously been filled with a virtual address.

Table 2-1 Network communication *(continued)*

Reference	Resolution
WP-2077	When multiple port redirects are created for Web Gateway to run as a High Availability proxy in Transparent Router mode, not only the one that was created last, but all of them appear in haproxy.cfg,
WP-2078	When Web Gateway runs as a High Availability proxy in Transparent Router mode, creating a port redirect with a space before the port number no longer causes the proxy to fail.
WP-2137	When Web Gateway is running as an High Availability proxy, the default timeout for client and server responses, which is set in /etc/haproxy/haproxy.cfg, has been increased to avoid frequent signing on and off.
WP-2141	Socks connections work again when Web Gateway is running as a High Availability proxy using virtual IP addresses.
WP-2143	When uploading a file from a client to a server over an active or passive FTP connection, the Proxy Protocol header gets no longer prefixed to the content data.
WP-2147	When Web Gateway runs in Transparent Bridge mode, enabling IP spoofing does not prevent HTTPS connections from working anymore.

Table 2-2 Web filtering and logging

Reference	Resolution
WP-1593	When bonded interfaces are in use on Web Gateway, IP addresses are again included in the names of the log files that record this use.
WP-1829	The haproxy log is no longer filled up with error messages after an issue with handling connections coming in at server downtime has been fixed. Performing log file rotation upon reaching a daily size limit is now sufficient to avoid an excessive log volume.
WP-2053	The var/log/ messages log is no longer flooded with entries generated by the ipmievd daemon to indicate that a certain fill level has been reached.
WP-2139	Processing Incoming requests on Web Gateway runs smoothly again after an issue with handling files compressed under gzip has been resolved.

Table 2-3 Vulnerabilities

Reference	Resolution
WP-1938, WP-2024, WP-2111, WP-2135	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2018-11784, CVE-2018-19519 • CVE-2019-0221, CVE-2019-2975 • CVE-2019-11729, CVE-2019-11745 For more information about each CVE and its impact, see the Red Hat CVE portal.

Table 2-4 Other

Reference	Resolution
WP-517	When a kernel failure happens, a core file for analysis is generated again as expected.

Resolved issues in the 9.0 release

This release resolves known issues.

JIRA numbers are provided in the reference columns of the tables below.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

Table 2-5 Network communication

Reference	Resolution
WP-1837	When web traffic is processed, external entities referenced in XML files are not resolved unintentionally anymore.
WP-1874	An infinite loop is no longer created when a CONNECT request that is submitted in HTTPS communication is forwarded.
WP-1941	When an initial TLS handshake has been completed in communication over secure connections, requesting a client certificate works as expected.
WP-1951	When a handshake is performed in communication that is secured under OpenSSL, enabling the option for allowing legacy signatures no longer prevents the use of elliptic curve algorithms and other newly introduced signature algorithms.
WP-2016	Processing HTTPS traffic works again when the Transparent Proxy mode with WCCP is configured, which had led to an issue when an option for allowing legacy signatures was enabled.

Table 2-6 Web filtering

Reference	Resolution
WP-1619	When ICAP traffic is processed in the embedded object cycle, filtering is only applied to the embedded object, having incorrectly included also the parent object before.
WP-1647	Auto-deleting older index directories from an anti-malware folder on Web Gateway works as expected.
WP-1811	When providing protection against threats arising from the use of web applications, the Facebook application name is handled properly in the filtering process.
WP-1826	When the URL to a web object includes a | (pipe symbol), the file opener no longer interprets this symbol as indicating an archive with embedded files.
WP-1865	When processing web traffic going on under HTTP2 results in blocking a download, the relevant blocking rule is displayed again on the progress page if any is used here.
WP-1954	When an attempt is made to import a certificate of a type that is not accepted on Web Gateway, error messages that misleadingly mention a whitelist restriction to account for the failure are not sent anymore.
WP-1871	Apps can be searched on Web Gateway using the catalog provided at the mobile,iron portal with Play Google being fully accessible, which it had not been previously due to a Safe Search conflict.
WP-1990	A file opening issue that led to a failure of the core process on Web Gateway has been fixed.

Table 2-7 Vulnerabilities

Reference	Resolution
WP-1938, WP-1956, WP-2009	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2016-3616 • CVE-2017-17742, CVE-2017-18267 • CVE-2018-1122, CVE-2018-6914, CVE-2018-8777, CVE-2018-8778, CVE-2018-8780 • CVE-2018-11212, CVE-2018-11213, CVE-2018-11214, CVE-2018-11784, CVE-2018-12910, CVE-2018-13988, CVE-2018-14348, CVE-2018-14498, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600, CVE-2018-14647, CVE-2018-15686, CVE-2018-15857, CVE-2018-16396, CVE-2018-16866, CVE-2018-16888, CVE-2018-19788 • CVE-2018-1000073, CVE-2018-1000074, CVE-2018-1000076, CVE-2018-1000077, CVE-2018-1000078, CVE-2018-1000079, CVE-2018-1000876 • CVE-2019-0221, CVE-2019-2949, CVE-2019-2975, CVE-2019-2989, CVE-2019-2999, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948 • CVE-2019-10181, CVE-2019-10182, CVE-2019-10185 For more information about each CVE and its impact, see the Red Hat CVE portal.

Table 2-8 Other

Reference	Resolution
WP-1474	A failure to initialize hardware monitoring sensors when a Web Gateway appliance is started does not occur anymore.

Rating for update 9.0.1

The rating defines the urgency for installing this update.

Recommended

Mandatory	Critical	High Priority	**Recommended**

- Recommended for all environments. Apply this update at the earliest convenience.
- Not applicable to hotfixes, because a hotfix is only created in response to a business-impacting issue.
- An update that resolves non-severe issues or improves product quality is considered as recommended.

For more information, see KB51560.

0C00