Revision J

McAfee Web Gateway 10.2.x Release Notes

Contents

What's new in the 10.2 release

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

McAfee® Web Gateway 10.2 is provided as a controlled release.

For information about how to upgrade to this release, see the Upgrading to a new version provided as a controlled release section of the *McAfee Web Gateway Installation Guide*.

Improvements for Proxy HA mode

Several options are now available that allow for improved performance and handling when running Web Gateway in Proxy High Availability (Proxy HA) network mode.

- An inactivity timeout, a load balancing algorithm, and sticky sessions can be configured, as well as egress IP addresses to increase the number of simultaneously active connections to cluster nodes scanning web traffic.
- Filtering traffic coming in under the SOCKS protocol is supported.

For more information, see the Proxy HA mode section of the *McAfee Web Gateway Product Guide*.

More protocol versions for secure ICAP

Different versions of the TLS and SSL protocols can now be selected when running Web Gateway in a secure ICAP server configuration.

For more information, see the ICAP server section of the *McAfee Web Gateway Product Guide*.

Property for troubleshooting ATD issues

The **Antimalware.MATD.Error.MessageDetails** string-type property has been added to the list of properties for use in web security rules. It provides details of an Advanced Threat Defense error message, such as timeouts, missing values, or network problems.

For more information, see the Properties - A section of the *McAfee Web Gateway Product Guide*.

More media types detected

More media types are detected by the functions for media type filtering on Web Gateway, including:

- Visio files with the following extensions: vsdm, vsdx, vssm, vssx, vstm, vstx
- CAD files

More efficiency in internal processing

Several internal processes have been improved on Web Gateway as follows.

- For users working with the WebSwing version of the user interface, the individual IP addresses of their client systems are recorded in the audit log when requests come in from these clients. The common 127.0.0.1 address is no longer in use here.

  This address had been logged for all users due the role as a remote desktop that WebSwing took from the point of view of the Java user interface.

  A commercial WebSwing version has also been implemented to overcome some limitations of the open source versions.
- More efficient methods of identifying customers, clients, and connections involved in issues that occurred are now used when reading core files stored in a temp folder.
- Some enhancements have been implemented for the consistency checking tool, which identifies unused settings and lists on Web Gateway.
- The feedback file that is evaluated on the master node in a cluster of Web Gateway appliances now provides the current version of the appliance software for each cluster node.
- Processing lists with entries in Regex format performs better due to an improvement of the diagnostic tool.

What's new in update 10.2.1

This release introduces several enhancements.

McAfee® Web Gateway 10.2.1 is provided as a controlled release.

SmartMatch optimization

Performance has been optimized for SmartMatch lookups by improving the way lists are handled when searching for matches.

Kerberos authentication with improved logging

When the Kerberos authentication method is used, error logging has been improved, for example, by writing client IP addresses in the log.

Handling of HTTP2 statistics improved

HTTP2 statistics, which are also shown on the Web Gateway dashboard, are provided under the Simple Network Management Protocol (SNMP) to be read by an external SNMP manage poll.

Resolved issues in update 10.2.8

This release resolves known issue.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.8 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*.

Resolved issue

JIRA issue number is provided in the reference column below.

Table 2-1 Vulnerabilities

Reference	Resolution
WP-4554	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2022-0778 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 10.2.7

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.7 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-2 Network communication

Reference	Resolution
WP-4451	The Bond interface is brought up with the appliance and Static Routes settings are restored correctly after a full restore of Web Gateway.

Table 2-3 Other

Reference	Resolution
WP-4134	A password for an update proxy user is escaped properly again, after this had not worked and caused yum to treat the user name as the name of the proxy server.
WP-4350	A URL path encoding issue that involved subscribed lists has been resolved.

Table 2-3 Other *(continued)*

Reference	Resolution
WP-4331	A 502 error that occurred when working with the AWS admin page has been resolved.
WP-4408	Java 1.8.0 openjdk is working normally.
WP-4440	An admin user can again log onto Web Gateway using NTLM authentication successfully.
WP-4450	The mwg-snmp.service unit is available again now after a reboot of Web Gateway.
WP-4444	Files are no longer detected as missing for Web Gateway nodes because of incorrect reference handling.
WP-4518	High memory usage on a Web Gateway appliance does not occur anymore.

Table 2-4 Vulnerabilities

Reference	Resolution
WP-4347, WP-4416	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2021-41617 • CVE-2021-4008, CVE-2021-4009, CVE-2021-4010 CVE-2021-4011 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 10.2.6

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.6 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-5 Network communication

Reference	Resolution
WP-3263	Traffic redirected to Web Gateway in Transparent Router mode is processed again.
WP-4255	A check status issue that happened when a handshake using TLS1.3 connection retries had not worked as expected due to a broken server connection has been fixed.
WP-4268	POST commands running while HTTP tunneling is enabled do not lead to a failure of the core process on Web Gateway anymore.
WP-4278	After deleting the haproxy.cfg manually, the haproxy functions work as expected.
WP-4328	Port redirection issues that occurred with range entries have been fixed.

Table 2-6 Web filtering and logging

Reference	Resolution
WP-3963	Web Gateway accepts incoming connections and continues to operate, which did not work after opening a corrupted .rar file.
WP-4061	Malicious Reputations use the ATD block template again.

Table 2-6 Web filtering and logging *(continued)*

Reference	Resolution
WP-4156	Invalid logon error "Session restricted to another IP" has been fixed.
WP-4270	Web Gateway now recognizes a Python 3.py script as python type,
WP-4271	TAR archives with Pax extended headers are recognized as allowed and no longer blocked.
WP-4279	System preference for an HTML-based user interface has been removed from the logon screen, so the Java-based user interface is available on the same terms.
WP-4330	PDF files are no longer blocked as corrupted media type when the "Block Corrupted MediaTypes" option is enabled under the Composite Opener.
WP-4369	A limit can be set to the compression ratio again after this had not been possible due to adding the "Body.MediaTypeFromHeader | Does not equal | <empty>" rule.
WP-4385	Logs can again be sent by SFTP.

Table 2-7 Other

Reference	Resolution
WP-3069	Bandwidth service is running normal after a Web Gateway upgrade.
WP-4071	High memory usage on a Web Gateway appliance does not occur anymore.
WP-4294	An MWG High CPU issue observed in multiple customer deployments has been fixed.
WP-4345	High memory usage when handling HTTP2 traffic does no longer occur.
WP-4379	An end-of-life version of log4j 1.x is not used anymore.
WP-4384	Luna HSM on 5500-E is running normal after a Web Gateway upgrade to 10.2.5.
WP-4404	Web Gateway 9.2.x and 10.2.x is successfully getting upgraded to 10.2.6 and 11.1 with quagga installed.

Table 2-8 Vulnerabilities

Reference	Resolution
WP-3335, WP-4131, WP-4159, WP-4197, WP-4237, WP-4259, WP-4329, WP-4348, WP-4355, WP-4376, WP-4407, WP-4421	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2021-43527 • CVE-2019-20892, CVE-2020-15862 • CVE-2021-35556, CVE-2021-35567, CVE-2021-35561, CVE-2021-35565, CVE-2021-35564, CVE-2021-35578, CVE-2021-35550, CVE-2021-35559, CVE-2021-35586, CVE-2021-35588, CVE-2021-35603 • CVE-2021-42574, CVE-2021-42694 • CVE-2021-20271 • CVE-2021-37750 • CVE-2021-22945, CVE-2021-22946, CVE-2021-22947 • CVE-2021-42373, CVE-2021-42373, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386 • CVE-2020-8927 • CVE-2021-44228, CVE-2021-45046 • CVE-2021-45105, CVE-2021-44832 • CVE-2021-4034 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 10.2.5

This release resolves known issue.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.5 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is not possible to configure any failover functions for these RADIUS servers.

Resolved issue

JIRA issue number is provided in the reference column below.

Table 2-9 Vulnerabilities

Reference	Resolution
WP-4355	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2021-44228 • CVE-2021-45046 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 10.2.4

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.4 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is not possible to configure any failover functions for these RADIUS servers.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-10 Network communication

Reference	Resolution
WP-3710	Web Gateway now supports intermediary headers in messages from HTTP2 -capable servers, so an HTTP2_PROTOCOL_ERROR no longer occurs here.
WP-4073	Bindings between protocol addresses and link layer addresses are established successfully while using an HTML GUI.

Table 2-11 Web filtering

Reference	Resolution
WP-3663	Web Gateway successfully retrieves reports from McAfee® Advanced Threat Defense regarding .zip files after sending a status query to Advanced Threat Defense.
WP-4158	The time consumed during a transaction can be retrieved again as a value for the **Timer.TimeInTransaction** property when Web Gateway is running as a proxy under TCP or the SOCKS protocol.
WP-4164	Files are no longer detected as corrupted under CPIO.

Table 2-12 Vulnerabilities

Reference	Resolution
WP-3806, WP-4203	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2021-31535 • CVE-2021-25214 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-13 Other

Reference	Resolution
WP-3247	The mcelog service will only be enabled on physical appliances now and will remain disabled on virtual appliances.

Resolved issues in update 10.2.3

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.3 is provided as a main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is not possible to configure any failover functions for these RADIUS servers.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-14 Network communication

Reference	Resolution
WP-4070	Performance issues that occurred when handling tunneled web traffic have been mitigated.

Table 2-15 Web filtering

Reference	Resolution
WP-4072	Performance is no longer impacted overmuch when many lists with SmartMatch entries are processed.

Table 2-16 Others

Reference	Resolution
WP-2686	Documents containing Austrian IBAN numbers are detected with the Data Loss Protection (DLP) functions on Web Gateway even if spaces between number groups are omitted.
WP-4022	The rsyslog daemon had kept the /var/log/haproxy/ haproxy-info_1.log file open until all disk space had been filled up on a Web Gateway appliance. This has been fixed now and log rotation works fine again.

Table 2-17 Vulnerabilities

Reference	Resolution
WP-3792, WP-4003, WP-4021, WP-4058, WP-4067	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2020-25649 • CVE-2021-2369, CVE-2021-2388 • CVE-2021-3520 • CVE-2021-3711, CVE-2021-3712 • CVE-2021-30640 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 10.2.2

This release resolves one known issue.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

This release, which is McAfee® Web Gateway 10.2.2, build 37835, is provided as the new main release.

For upgrade information, see Upgrading to a new version provided as a main release in the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is not possible to configure any failover functions for these RADIUS servers.

Resolved issue

The JIRA issue number is provided in the reference column below.

Table 2-18 Logging on

Reference	Resolution
WP-4043	Admins can log on to the Web Gateway user interface again from external accounts.

Resolved issues in update 10.2.1

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.2.1 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is currently not possible to configure any failover functions for these RADIUS servers.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-19 Network communication

Reference	Resolution
WP-1455	POST commands run while HTTP tunneling is enabled do not lead to a failure of the core process on Web Gateway anymore.
WP-3810	When a director node is not working as a scanner in a Proxy High Availability (Proxy HA) configuration, the proxy on Web Gateway listens to other scanning nodes again.

Table 2-20 Web filtering and logging

Reference	Resolution
WP-3072	Only errors relating to the user interface are logged in the mwg.ui.errors log, whereas unexpected errors, such as error 143 and others, are not logged anymore.
WP-3658	When uncategorized URLs are blocked, events are successfully synchronized for two Trusted Source properties, which had not worked properly before, as an unexpected event had been added.
WP-3751	Upgrade packages for Web Gateway can be downloaded, which had not been possible because the PGP key files inside these packages were blocked as encrypted media types.

Table 2-20 Web filtering and logging *(continued)*

Reference	Resolution
WP-3811	Requests to retrieve CRL and OSCP information about the status of certificates used for secure communication are forwarded, which had not worked in a next-hop proxy chain with two Web Gateway appliances.
WP-3903	Log file pushing works again after logging a switch to a supported repository version with mwg-switch repo, which had failed before, as no permission to read the log files was reported as an error.
WP-3904	Infinite loops, which caused threads to hang and resulted in problems with high CPU and memory load, are no longer created when zip archives are scanned.

Table 2-21 Vulnerabilities

Reference	Resolution
WP-3468, WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934, WP-3935, WP-3936, WP-3999	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2016-3674 • CVE-2017-7957 • CVE-2017-11610 • CVE-2019-10208 • CVE-2020-24489, CVE-2020-25111, CVE-2020-25112, CVE-2020-25113, CVE-2020-25648, CVE-2020-25694, CVE-2020-25695, CVE-2020-26217 • CVE-2021-3472 • CVE-2021-21341, CVE-2021-21342, CVE-2021-21343, CVE-2021-21344, CVE-2021-21345, CVE-2021-21346, CVE-2021-21347, CVE-2021-21348, CVE-2021-21349, CVE-2021-21350, CVE-2021-21351 • CVE-2021-22876, CVE-2021-22890, CVE-2021-22901 • CVE-2021-25217 • CVE-2021-27219 • CVE-2021-32027 • CVE-2021-33909 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in the 10.2 release

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

Review also the following additional information.

HSM firmware upgrade

If the Hardware Security Module (HSM) firmware you are using is not compatible with the new 12.60 HSM driver version, you must obtain the required firmware version from the vendor and perform a firmware upgrade before upgrading to a new version of the Web Gateway appliance software. The vendor is Entrust.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-22 Network communication

Reference	Resolution
WP-2823	Long-running web socket connections last again as expected after terminating prematurely before and the configured timeout is observed.
WP-3274	More than 15 ports can be specified for a port redirection rule, which had not worked before, but is handled now by creating additional IP tables.
WP-3303	When Web Gateway runs as a web proxy in Proxy High Availability (HA) mode, processing requests for web access that come in from clients under FTP, the virtual IP address (VIP) sent initially to a client used to be replaced with a different VIP upon directing the request to a scanning node in passive FTP mode, which caused the process to fail, as the client was unaware of the changed VIP. The VIP now used by a Web Gateway appliance when connecting as director node to an appliance that runs as scanning node in passive FTP mode is the one that is configured as VIP of the Virtual Router Redundancy Protocol (VRRP) interface. When more than one VIP is configured for this interface, the most recently added is used. This applies to a Proxy HA as well as to a Transparent Router setup.
WP-3440	When Web Gateway runs in Proxy High Availability (Proxy HA) mode, log files are rotated in a suitable manner preventing overflow of the Proxy HA log and spilling over into other partitions, which had happened before.
WP-3529	When stickiness is configured for forwarding requests for web access from a client to a particular next-hop proxy, this is observed again after not having worked properly before.
WP-3540	When Web Gateway runs as proxy, a virtual IP address can be configured and used as the proxy IP address, which had not worked as expected.
WP-3585	A certificate for secure connections can be removed along with its certificate chain and a new certificate implemented without the old chain still showing up in vulnerability scans.
WP-3631	When several appliances run in Proxy High Availability (Proxy HA) network mode, the load balancer distributes work load only to ports on nodes that have been entered in the scanner table whereas all ports in the HTTP proxy table had been considered before due to a faulty line in a configuration file.
WP-3639	In a Proxy High Availability (Proxy HA) setup only one node is shown with active director status at a time, whereas two were shown before even though only one had really been acting as director node.
WP-3787	When static routes are configured, the tool tip message no longer suggests that the field for the gateway IP address might be left empty, which is actually not allowed here.

Table 2-23 Authentication

Reference	Resolution
WP-3555	After sending a connect request to a domain controller for authentication under NTLM, Web Gateway checks the size of the response and reads the data as expected after having thrown an out-of-range exception before, which was due to an unsuccessful attempt to read the hardcoded response length from the buffer.
WP-3612	When user group information is evaluated for authentication purposes in a cluster of Web Gateway appliances, Chinese characters in the name of a user group are read without problems everywhere in the cluster. This had not worked before, as these characters were read properly on one cluster node, but when group names were distributed to other nodes running as proxies, authentication failed because these characters could not be read there.
WP-3678	When authentication is performed using the NTLM authentication method, moving a user name to a different group can be done with domain information showing up properly in the group name. The domain shown before in the name of a group after moving a user name there was the domain of the group the user had previously belonged to. Now it is the current domain, where the group is located that the user has been moved to.

Table 2-24 Web filtering

Reference	Resolution
WP-3384	When required values are missing in responses Advanced Threat Defense sends to Web Gateway, this is reported in an error message, whereas only a communication failure had been reported before. The error is also returned when the **Antimalware.MATD.Error.MessageDetails** property is processed.
WP-3617	Encrypted files that are processed on Web Gateway are detected and blocked under a rule that is configured after having been allowed before or blocked not as encrypted, but due to their file types, which were mistakenly recognized as unknown.
WP-3674	When a block rule is configured in URL filtering, it blocks requests matching the blocking criteria and is no longer impacted by requests originating under the Periodic Rule Engine Trigger, which had stopped the request cycle before this block rule could be processed.
WP-3714	When Web Gateway uses a Hardware Security Module (HSM) solution, storing private keys in the HSM Agent folder works as expected after having led to errors before.

Table 2-25 Vulnerabilities

Reference	Resolution
WP-2788, WP-3445, WP-3483, WP-3484, WP-3527, WP-3528, WP-3547, WP-3577, WP-3579, WP-3581, WP-3584, WP-3589, WP-3611, WP-3744, WP-3745, WP-3746, WP-3747, WP-3793, WP-3800	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2016-3088 • CVE-2016-6810 • CVE-2014-114 • CVE-2019-10086 • CVE-2019-25013 • CVE-2020-1957 • CVE-2020-8625 • CVE-2020-10029, CVE-2020-10543, CVE-2020-10878 • CVE-2020-12321, CVE-2020-12723 • CVE-2020-14347, CVE-2020-14360, CVE-2020-14372 • CVE-2020-25632, CVE-2020-25647, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25712 • CVE-2020-27749, CVE-2020-27779 • CVE-2020-29573 • CVE-2020-36221, CVE-2020-36222, CVE-2020-36223, CVE-2020-36224, CVE-2020-36225, CVE-2020-36226, CVE-2020-36227, CVE-2020-36228, CVE-2020-36229, CVE-2020-36230 • CVE-2020-110224 • CVE-2021-2161, CVE-2021-2163 • CVE-2021-3347, CVE-2021-3449, CVE-2021-3450 • CVE-2021-20225, CVE-2021-20233, CVE-2021-20305 • CVE-2021-23839, CVE-2021-23840, CVE-2021-23841, • CVE-2021-25215, CVE-2021-25216, CVE-2021-25329 • CVE-2021-27135 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-26 Other

Reference	Resolution
WP-1232	Chinese characters can be entered on the user interface with the Microsoft Input Method Editor (IME), which is provided as part of the relevant language pack by Microsoft. This applies also to Japanese characters and others that are entered with the IME tool.
WP-3564	Log files can be pushed to a log that uses spaces in the name of the log folder after spaces in the folder name had led to an error before.
WP-3591	A timeout that is set for deleting content stored under a PD storage rule is observed and the content deleted completely, which had only worked for parts of the content before.
WP-3694	A missing nscd package is now included in upgrading Web Gateway, which avoids an upgrade failure due to nscd dependencies that cannot be met preventing also glibc and other dependent upgrades.

Rating for update 10.2.8

The rating defines the urgency for installing this update.

This release is recommended for all environments. Apply this update at the earliest convenience.

0J00

McAfee