Release Notes Version 12.2

https://campus.barracuda.com/doc/100370866/

Please Read Before Updating

Before updating to a new firmware version, be sure to back up your configuration and read the release notes for each firmware version that you will apply.

Do not manually reboot your system at any time during an update, unless otherwise instructed by Barracuda Networks Technical Support. The update process typically takes only a few minutes to apply. If the process takes longer, please contact Barracuda Networks Technical Support for assistance.

SSL certificates signed using weak hashing algorithms such as MD5 and SHA1 are not supported with OpenSSL 3.0. Ensure that all existing certificates signed with MD5 and SHA1 are replaced with SHA-256 signed certificates before you upgrade to 12.2.0.x. If an upgrade is performed without replacing these certificates, services using them will go down and rollbacks occur. [BNWF-55392]

Fixes and Enhancements in 12.2

Advanced Bot Protection

Features and Enhancements:

- **Client Fingerprint Cookies :**
  - Any tampering of the Client Fingerprint cookie values is now detected and blocked [BNWF-55005].
  - An option is provided on the web interface to enable the Fingerprint cookie mechanism for all services that serve the subdomains of the domain of the service. This is enforced only when **Enable Client Fingerprint** is also set to **Yes**.[BNWF-54903]
- **Geo IP Region List:** Kosovo and Curaçao have been added to the Geo IP regions list. [BNWF-55371] [BNWF-55142]

Fixes:

- **Fix**: The **Bot Statistics** section on the Advanced Bot Protection dashboard now displays the hyperlinks. [BNWF-55010]
- **Fix**: A datapath outage issue caused by the Fingerprinting module has been fixed.

[BNWF-55932]

Security

Feature

- Extended the support for deep inspection of files uploaded through mechanisms that are beyond multipart content type using the POST method.
  - Files uploaded through application/octet-stream using POST methods are now subjected to virus scanning and MimeType checks. [BNWF-27840]
  - Files uploaded through multipart-formdata and application/octet-stream using the PUT method are subjected to virus scanning and MimeType checks. [BNWF-53609]
- Data theft exception patterns can now be added to a URL policy on the **BOT MITIGATION > Bot Mitigation** page, **Bot Mitigation** section. [BNWF-54996]

Enhancements:

- **TLS defaults**:
  - TLS 1.3 is enabled by default for new servers and rule group servers. [BNWF-55435]
  - TLS 1.1 is disabled by default for new SSL services, servers, and rule group servers. [BNWF-55128]

Fixes:

- **Vulnerability Fix**: HTTP/2 Rapid Reset Attack vulnerabilities mentioned in CVE-2023-44487 has now been fixed. [BNWF-55472]
- **Fix**: The datapath crash due to an attack exploiting the permissible value length in OpenID Connect is now fixed. [BNWF-55265]
- **Fix**: Creating a new rule group using the template no longer copies the original name of the rule group. [BNWF-52774]
- **Fix**: An intermittent issue where valid requests were being blocked and not redirected after solving a CAPTCHA challenge has been fixed. [BNWF-54330]
- **Fix**: If the credential stuffing attack is detected in the request when the service is in **Active** mode and the URL policy associated with the service is set to **Passive**, the attack is now logged on the **BASIC > Web Firewall Logs** page. [BNWF-54329]
- **Fix**: Datapath outage due to the tampered fingerprint cookie has been fixed. [BNWF-55737]
- **Fix**: A rare outage caused by a race condition in the brute force checks has been fixed. [BNWF-55660]
- **Fix**: The issue in SSL processing modules when the Barracuda Blocklist feature is enabled has been fixed. [BNWF-55614]

System

Deprecation Notice:

- FTP and FTP SSL service types will not be supported starting with the next major firmware release. Also, any existing FTP/FTP SSL services configured on the **BASIC > Services** page will be disabled. [BNWF-55679]

- Older cryptographic protocols with low-security levels (SSLv3, TLS 1.0, and TLS 1.1) will not be supported on the Barracuda Web Application Firewall starting with the next major firmware release.

Weaker protocols will not be supported when configuring new services. For existing services, clients will be unable to establish the connection using the deprecated protocols. Administrators are requested to review the configuration and make this change if required. [BNWF-55818]

Enhancements:

- You can now show certificates that are 'Expiring in 30 days' on the **BASIC -> Certificates** tab. [BNWF-54640]
- **OpenSSL version**: OpenSSL version has been updated to 3.0.9. [BNWF-54852]

Fixes:

- **Fix**: An issue where the firmware was not being downloaded and applied if the proxy settings were configured has been fixed. [BNWF-55044]
- **Fix**: An issue where SNMPv3 was crashing in certain scenarios when the service had 'Compression' enabled has been fixed. [BNWF-54329]
- **Fix**: Users with 'accent' characters in their LDAP server username can now log in. [BNWF-54705]
- **Fix**: The broken Country link in the Online Help section of **BASIC > Web Firewall Logs** has been fixed. [BNWF-53590]
- **Fix**: Traffic with a large number of parameters in requests can now be processed. [BNWF-55615]
- **Fix**: An error in handling malformed requests has been fixed. [BNWF-55613]
- **Fix**: A rarely observed data path outage in the Caching module has been fixed. [BNWF-55611]
- **Fix**: An issue with uploading a Trusted CA certificate on the **ADVANCED > Secure Administration** page has been fixed. [BNWF-55929]

API Security

Enhancements:

- **JSON Profiles**
  - JSON profile REST API now supports strict-check, extended-match-sequence, and extended-match parameters. [BNWF-55485]
  - JSON URL profile now supports **Allowed Methods**. [BNWF-55124]
  - JSON key profile "MAX Length" can now support up to 256k data. [BNWF-50203]

    The max value length for the JSON key value is 8192 with the JSON policy. If a request has a key that exceeds the max value length, the request will be blocked. To allow more than 8192 bytes of value length, it is recommended to create a key profile and adjust the max value length in the profile.
  - The hash (#) character is allowed in JSON key names. [BNWF-54723]
- **JSON Profile Extended Match**
  - When a new service is created, the default JSON profile **Extended Match** uses a wildcard (*) to match with the incoming requests. [BNWF-55460].

Fixes:

- **Fix**: The Maximum Upload Files is set to null (0) if the Content-Type of an endpoint is 'application/json'. [BNWF-54546]
- **Fix**: The datapath outage issue that was observed when sending JSON data with a key length greater than 1 MB in size has been fixed. [BNWF-55838]
- **Fix**: The Maximum Upload Files on the **WEBSITES > URL Profiles** page now display the configured value [BNWF-55955].
- **Fix**: You can now add multiple exception patterns when creating a JSON key profile. [BNWF-54521].
- **Fix:** An issue where a false positive was being triggered when the 'Open API Spec import' feature implicitly creates a Form Spam profile has been fixed. [BNWF-54884]
- **Fix**: An issue with REST API validation that allowed users to configure IPv6 addressing even when the setting was disabled under **Basic > IP Configuration** has been fixed. [BNWF-32441]

High Availability

Fixes:

- **Fix**: In HA, the deletion of CRL files in one system is now synchronized with all systems in the cluster. [BNWF-55001].

Logs and Reports

Fixes:

- **Fix**: An issue where the Attack Details section in the Web Firewall Logs was getting truncated if it contained multiple violations has been fixed. [BNWF-54806]

Cloud

Feature:

- **Public Cloud Rebranding** - WAF images on public cloud platforms have been rebranded as "Web Application Firewall". [BNWF-54906]