Release Notes Version 12.0

https://campus.barracuda.com/doc/96773488/

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.

Fixes and Enhancements in 12.0

Client-Side Protection

- **Feature**: Ability to configure/fine-tune CSP policy from the ATI dashboard. Provides more control over violations and supports configuration actions from the ATI dashboard. [BNWF-50034]

Security and Access Control

- **Feature**: The Barracuda WAF now provides support to enable a Cross-Origin Resource Sharing (CORS) option for back-end applications. [BNWF-48893]
- **Feature**: In OpenID Authentication on ADVANCED > Admin Access Control > External Authentication Services, administrators can now configure "Allowed Users" and enable access to the web application only to the specified users. [BNWF-48852]
- **Feature**: The Barracuda WAF now allows users to block requests based on their Autonomous System Numbers (ASN). You can configure ASNs at the application layer IP Reputation and block the request originating from those ASNs. [BNWF-46039]

Fixes and Enhancements

- **Enhancement**: Mitigations for HTTP request smuggling attacks is now also taken care of for non-POST methods. [BNWF-51004]
- **Enhancement**: The SameSite attribute can now be configured from the Cookie Security page. By default, this attribute will not be added by the WAF. It can be configured later to either Lax/Strict/None. [BNWF-45679]

- **Enhancement**: Fingerprint risk score computation framework improved to ensure that upstream load balancers in cloud deployments are not blocked. [BNWF-49259]
- **Fix**: Datapath crash seen after reconfiguring “Exception Patterns” for a URL profile has been fixed. [BNWF-51620]
- **Fix**: An empty space after 'Cookie:' was causing the WAF to insert '=' when forwarding the same request to the back-end server. This has been resolved. [BNWF-51580]
- **Fix**: A configuration scenario that allowed the deletion of a certificate that is being used as the client certificate for client authentication in one of the Content Rule Servers has been fixed. [BNWF-51355]
- **Fix**: A bug in the back-end SSL flow, which resulted in data-path outages, has been fixed. [BNWF-51336]
- **Fix**: A datapath crash was observed when Rate Control was enabled. This issue has been fixed. [BNWF-51679]
- **Fix**: An issue that caused frequent datapath crashes when using the Advanced Bot Protection (ABP) module has been fixed. [BNWF-51198]
- **Fix**: A SAML relay state truncation issue due to a large relay state URL has been fixed. [BNWF-50930]
- **Fix**: Configuration rollback was observed when creating a JWT profile with the URL match. This issue has been fixed. [BNWF-50700]
- **Fix**: An issue with a special character in the LDAP password has been fixed. [BNWF-50660]
- **Fix**: The parameter name/value pair in requests originating from trusted hosts are now processed without enforcing attack checks. [BNWF-50091]
- **Fix**: An issue that caused Exception Learning to create URL profiles with empty values has been fixed. [BNWF-50041]
- **Fix**: Bruteforce is now enabled when Credential Spraying is enabled using REST API v3.x. [BNWF-49258]
- **Fix**: Web Firewall Logs now display the correct attack name and attack type. [BNWF-24155]
- **Fix**: In case of a 302 response code with 0-Byte data, the WAF marked the response type as Internal in the Access logs. This issue has been fixed. [BNWF-12531]
- **Fix**: An issue in the back-end SSL flow that resulted in datapath outages has been fixed. [BNWF-51336]
- **Fix**: An authentication module datapath crash on parsing Russian unicode characters has been fixed. [BNWF-51124]
- **Fix**: An OpenID datapath crash on simultaneous login of multiple users has been addressed. [BNWF-48803]
- **Fix**: An issue where the request URLs in the Authentication module were trimmed off after the standard extension (Example: .exe, .cgi) has been resolved. [BNWF-49753]
- **Fix**: A datapath crash observed in OpenID Connect when handling requests with more than 16 headers has been fixed. [BNWF-51345]
- **Fix**: Intermittent OpenID datapath crashes in some error condition has been addressed. [BNWF-50204]
- **Fix**: A possible outage when parsing cookies that arrive in a specific condition has been addressed. [BNWF-50960]
- **Fix**: An issue with masking sensitive data with two or more consecutive parameter separators, like ampersand, has been addressed. [BNWF-50192]
- **Fix**: A possible race condition leading to an outage when the instant SSL feature is enabled has

been fixed. [BNWF-49762]
- **Fix**: A possible condition in which the worker processes continuously consume more resources when looking through the bruteforce-related bookkeeping measures has been fixed. [BNWF-49622]

Traffic Management

Fixes and Enhancements

- **Enhancement**: In the Request/Response rewrite rule, headers that appear multiple times and match the criterion are honored and all corresponding headers are modified. [BNWF-48824]
- **Fix**: Large sites can now be downloaded without any issue when HTTP2 is enabled on the service level. [BNWF-50981]
- **Fix**: An outage in ActiveSync has been addressed. [BNWF-50770]
- **Fix**: An issue with the networking rules after manufacturing a WAF on very specific hardware models (964D/861C) has been addressed. [BNWF-50017]
- **Fix**: Sanitized rate control outage handling when HTTP2 is now enabled. [BNWF-49712]
- **Fix**: An issue with the destination NAT rule table header has been fixed. [BNWF-51644]

System Management

- **Feature**: Attacks on the BASIC > Dashboard can be clicked to filter the logs based on the selected attack type. [BNWF-49742]
- **Feature**: Ability to show/hide all attack graphs using a single click. [BNWF-49743]
- **Feature**: The ADVANCED > Admin Access Control page provides the ability to grant role-based administration access to perform the configured actions on the ATI dashboard. [BNWF-50137]
- **Feature**: The WAF management web server is now upgraded to the latest stable version to address multiple security vulnerabilities. [BNWF-51348]
- **Feature**: Intercom is now integrated in the Barracuda WAF web interface. The intercom service communication is enabled by default. [BNWF-50734]

Fixes and Enhancements:

- **Enhancement**: The tolerance for the config process hang check monitors has been increased to prevent a possible false positive. [BNWF-50952]
- **Enhancement**: The country code for Gibraltar has been added to the country list in the IP Reputation Geo Pool. [BNWF-46801]
- **Enhancement**: It is now possible to export country code information to the syslog servers. [BNWF-50604]
- **Enhancement**: An expandable menu has been added on the BASIC > Dashboard page to display Notices and Warnings. Users are now provided with the expand and collapse options to view and hide the list of notices/warnings. [BNWF-51327]

- **Enhancement**: "Internal Attack Patterns" can now be configured using REST API v3.x. [BNWF-50741]
- **Fix**: A possible false positive that resulted in the monitor processes bringing down the data path due to multiple instances has been fixed. [BNWF-51391]
- **Fix**: Uploading a trusted certificate on the ADVANCED > Secure Administration page no longer resets the supported SSL protocols that are allowed to access the WAF GUI. [BNWF-51390]
- **Fix**: It is now possible to create a certificate using the Safari browser without any issues. [BNWF-51025]
- **Fix**: Memory issues with the datapath process when Client Fingerprinting was used has been fixed. [BNWF-51016]
- **Fix**: Multiple issues with the 'GeoIP Allowed/Blocked networks' templates has been fixed. [BNWF-50979]
- **Fix**: An issue that prevented users from changing the HTTPS port used to access the WAF GUI has been fixed. [BNWF-50730]
- **Fix**: An outage due to custom header logging when handling the server response has been fixed. [BNWF-50111]
- **Fix**: An issue with deleting a saved configuration backup has been fixed. [BNWF-51209]
- **Fix**: Let's Encrypt renewed certificates can now be associated to a service with the service name in capital letters. [BNWF-48524]
- **Fix**: SNMP memory is now monitored, and appropriate actions are being taken. [BNWF-47506]
- **Fix**: The Application Summary report on the BASIC > Reports page now displays the Rule Group Server and Port information. [BNWF-47492]
- **Fix**: A possible false positive that resulted in the monitor processes bringing down the data path due to multiple instances of a datapath being detected has been fixed. [BNWF-51391]

API Security

- **Feature**: Automatic discovery for API endpoints and structure learning that provides ease of use for configuring API security is now available for systems with an active ATI subscription. [BNWF-50871]
- **Feature**: The Barracuda WAF now provides native parsing, security, and delivery of applications with GraphQL APIs. [BNWF-49082]

Fixes and Enhancements:

- **Fix**: JSON security now validates max array elements. [BNWF-50731]

Account Takeover Protection

- **Feature**: Account profiling implemented for privileged account protection. [BNWF-50131]