# Barracuda WAF 12.2 Firmware Hardened to Augment Security of Product Features

https://campus.barracuda.com/doc/112168286/

It is recommended to upgrade firmware to 12.2 GA to provide augmented feature functionality in 11.x, 12.0 and 12.1 firmware.

**Description**: This advisory is only applicable for the Web Applications utilizing the following features and the application is in “Active Block mode”.

1. The web application requires an HTTP method other than POST to upload a file. The **File Upload Protection** feature provides the default security policy that allows only the POST method. However, users can override the default policy and add other HTTP methods. As per the feature coverage in 11.x, 12.0 and 12.1 firmware, the newly added HTTP methods will not be deep inspected. This product feature coverage may render “File upload protection (Antivirus protection - ATP module)” ineffective for HTTP methods other than POST.
2. To prevent the JSON security protection settings from being bypassed if the default security policy is edited to include an HTTP method that is not specifically set in the JSON security policy, the web application now includes an HTTP method other than POST for JSON payloads.

Please examine the below mentioned workflows to harden the security posture as applicable to your web application.

| Feature Gap | Affected Firmware Version | Fixed Firmware Version |
|---|---|---|
| Category 1: Augment File upload protection | 11.x<br>12.0<br>12.1 | 12.2 |
| Category 2: Augment security of JSON security module | 11.x<br>12.0<br>12.1 | 12.2 |

## Advisory Category 1

The Category 1 documents feature descriptions and associated effects in the file upload protection feature of the Barracuda Web Application Firewall. It was discovered that the file upload protection security settings can be bypassed if an HTTP method other than POST is used. The PUT method can be used to create (upload) or change resources on a target system. When using the PUT method, the file upload security policies and restrictions can be circumvented and be used to upload malicious files, trigger RCE vulnerabilities, or chain LFI vulnerabilities. This may result in the PUT request bypassing security settings and protection mechanisms.

- This advisory is applicable ONLY if you have allowed the PUT method in the IDs mentioned in Category 1.
- The PUT method is not allowed by default.

Following are the IDs for Advisory Category 1:

- ID 1.1
- ID 1.2
- ID 1.3
- ID 1.4

#### ID 1.1

**Description**: Using the PUT method and uploading multiple files in one request can bypass the "Max Allowed Files" count set on the WAF.

If the WAF administrator limits the number of files that can be uploaded onto a protected web application to 0, but is not limited to the need to protect an existing upload vulnerability present on a backend system, the security policy can be bypassed by using a method like PUT.

#### Recommended Action

1. Upgrade to 12.2 GA.
2. After the upgrade, configure **Maximum Upload Files** to the required value as per the application.
3. The recommended value is **5**.

#### ID 1.2

**Description**: Using a method other than POST can bypass the security settings that limited the allowed MIME file types set on the WAF.

If the WAF administrator limits the MIME types allowed to be uploaded to an application to protect which executables can be uploaded (which can lead to, for example, RCE and/or CFI vulnerabilities being exploited), the protection measures can be bypassed by using a method like PUT.

### Recommended Action

1. Upgrade to 12.2 GA.

#### ID 1.3

**Description**: Using a method other than POST can bypass the associated antivirus engine.

If the WAF administrator protects a backend application from the ability to upload malicious files by using the antivirus engine provided, the protection measures can be bypassed by an attacker by using a method like PUT.

**Recommended Action:**

1. Upgrade to 12.2 GA.

**ID 1.4**

**Description**: Using a method other than POST can, under certain circumstances, bypass the BATP engine.

If the WAF administrator protects a backend application from the ability to upload malicious files by using the Barracuda Advanced Threat Protection engine provided, the protection measures can be bypassed by an attacker by using a method like PUT.

**Recommended Action:**

Users subscribed to ATP can request a support-assisted firmware patch.

## Advisory Category 2

The Category 2 documents feature descriptions and associated effects in the JSON security protection module of the Barracuda Web Application Firewall. It was discovered that the JSON security protection settings can be bypassed if an attacker changes to an HTTP method that is not specifically set in the JSON security policy.

The Barracuda Web Application Firewall provides a default JSON security policy that is., set to POST methods by default. In the Website Profiles settings, setting the methods results in limiting the methods to those set in the policy. Other methods would then be blocked. The method settings in the JSON security policies work as matching criteria. This results in the payload body to be passed to the backend system, thereby possibly bypassing failsafe check mechanisms if the method does not match the settings in the policy.

Following are the IDs for Advisory Category 2:

- ID 2.1
- ID 2.2
- ID 2.3

**ID 2.1**

**Description**: Using the API specification upload feature on the WAF can cause insufficient protection of the API endpoints set.

If an administrator uploads an API specification file, such as an Open API Schema (OAS)/Swagger specification, endpoint policies are successfully set, but the method matching criteria on the created policies get set as the one defined on the API specification. Methods other than the one defined on the policy malicious payload can be transferred to the backend, thereby possibly bypassing the policy conformance check.

**Recommended Action:**

1. Upgrade to 12.2 GA.

**ID 2.2**

**Description**: Using the API specification upload feature on the WAF may result in insufficient protection of API endpoints not set by the WAF.

If an administrator uploads an API specification file, such as an OAS/Swagger specification, endpoint policies are successfully set, but no "last resort" policy is set by the WAF to protect endpoints that were not present in the OAS. If an attacker were to send a malicious payload to an endpoint other than the ones present in the OAS, a malicious body payload is transferred to the backend, thereby possibly bypassing security checks.

**Recommended Action:**

1. Upgrade to 12.2 GA
2. After the upgrade, it is recommended that you follow the manual configuration steps.
3. Set **Extended Match** to ***** from **Method eq POST** for the default JSON profile.

**ID 2.3**

**Description**: The default JSON security policy set by the WAF provides protection only for JSON payloads coming over the POST method.
This product design may result in the parsing process being bypassed in the absence of a global failsafe mechanism. This would limit the efficacy of the WAF security policy.

**Recommended Action:**

1. Upgrade to 12.2 GA
2. After the upgrade, it is recommended that you follow the manual configuration steps.
3. For all existing JSON profiles on the **WEBSITES > JSON Security** page, **JSON Security**

section:

4. Set **Extended Match** to *.
5. Enable **Strict Method Check**.
6. Set **Allowed Methods** to only those required by the JSON payload for the API endpoints.

For any assistance or questions regarding this advisory, contact Barracuda Networks Technical Support.