contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Barracuda Networks Multiple Products exploited

CVE-2026-111560 · on CISA's exploited list since 10 November 2026

Analysis Report

Anyone running Barracuda ESG, Load Balancer ADC, WAF, WSG, Message Archiver or WAF Control Center must apply the vendor's patches by 13 November 2026. If you do not run these appliances, nothing to …

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 7.2**	STATUS	On CISA's exploited list; due 13 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/barracuda-networks-multiple-products-cve-2026-111560

The bottom line

> *Anyone running Barracuda ESG, Load Balancer ADC, WAF, WSG, Message Archiver or WAF Control Center must apply the vendor's patches by 13 November 2026. If you do not run these appliances, nothing to do; otherwise restrict the Admin UI to internal networks and apply the named patches immediately.*

At a glance

Fact	Detail
Product	Barracuda Networks Multiple Products (CVE-2026-111560)
Severity	High: 7.2 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 13 November 2026.
Chance of exploitation (EPSS)	0.09, the estimated chance in the next 30 days, as at 13 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	ESG: patches BNSF-40425 (firmware 9.4.017 and above) and BNSF-40430 (below 9.4.017); ADC and WAF: BNADC-16586; Message Archiver: BNMA-32468; WAF Control Center: BNWF-60060; WSG: BNYF-24789.
Who looks first	Organisations running Barracuda ESG, Load Balancer ADC, WAF, or WSG. The vendor's advisory also names Message Archiver and WAF Control Center as affected by this CVE; the CVE record does not list those two.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any Barracuda ESG, ADC, WAF, WSG, Message Archiver or WAF Control Center?	Nothing to do for this CVE.	Check the current firmware version and patch status of each appliance.
Are the named patches for your products applied?	Apply the relevant patch immediately; contact Barracuda Support if needed.	Check whether the Admin UI is accessible from outside your internal network.

Is the Admin UI accessible from outside your internal network?	Exposure is reduced; confirm patches are in place.	Restrict Admin UI access to internal networks now, then apply patches.

What it is

An authenticated administrator can enter a crafted timezone value in the appliance's configuration. The record says that value is later processed in a way that lets injected operating system commands run with root privileges on the device.

Why it matters

The flaw requires an administrator account on its own. On ESG it chains with CVE-2026-116606, a pre-authentication bypass the vendor's advisory covers in the same release; together they allow an attacker with Admin UI access to reach root without valid credentials. The advisory says exploitation has been observed at a small number of organisations. For other products, an attacker must already hold admin credentials. Our reading is that ESG with an internet-facing Admin UI is the highest-risk configuration and warrants the same urgency as an unauthenticated flaw.

What the vendor's advisory says

We read one page on trust.barracuda.com. In short:

- The same advisory covers CVE-2026-116606, a pre-authentication authorization bypass affecting ESG (High severity). The two CVEs together could allow an attacker to bypass authorisation and obtain root on the device.
- The advisory says exploitation activity has been observed at a small number of organisations. It recommends restricting the Admin UI to trusted internal networks and enabling automatic patching.

Things people will get wrong

- Only the Email Security Gateway is at risk here The CVE record lists ESG, Load Balancer ADC, WAF, and WSG as affected. The vendor's advisory adds Message Archiver and WAF Control Center; the record does not list those two.
- No login is needed to exploit this vulnerability The record says exploitation requires an authenticated administrator. An unauthenticated path exists only if CVE-2026-116606 is also exploited on ESG and the Admin UI is reachable.

The wording includes conditions the score may not show: it needs privileges; the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find which Barracuda appliances you run and their firmware versions

- Log in to each appliance's management interface and note the current firmware version shown on the status or system information page.
- Check whether automatic patching is enabled; the vendor's advisory says the device will show the latest firmware version available.

Step 2: Check whether the Admin UI faces the internet

- Review firewall rules for the management port of each appliance to confirm whether it is reachable from outside your internal network.
- The vendor's advisory says organisations whose Admin UI is not publicly accessible are less exposed to this attack path.

Step 3: Apply the named patches for each affected product

- Apply the patch for your product: BNSF-40425 or BNSF-40430 for ESG; BNADC-16586 for ADC and WAF; BNYF-24789 for WSG; BNMA-32468 for Message Archiver; BNWF-60060 for WAF Control Center.
- If a device's firmware is several versions out of date, the advisory says more than one update may be needed; contact Barracuda Support for assistance.

Step 4: Confirm patches are in place and Admin UI access is restricted

- Return to the management interface and verify the patch status matches the applied patch ID.
- Confirm the Admin UI is reachable only from trusted internal addresses.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We run Barracuda appliances and need to confirm our exposure to CVE-2026-111560, an OS command injection flaw affecting ESG, Load Balancer ADC, WAF, WSG, and, per the vendor's advisory, Message Archiver and WAF Control Center. The CISA remediation deadline is 13 November 2026. The vendor has issued named patches for each product. Please confirm: which of these appliances we have deployed, the current firmware version of each, whether the named patches are applied, and whether the Admin UI is accessible from outside our network. We would like written confirmation of the firmware version and patch status as soon as possible.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected changes to the timezone configuration in appliance settings — the record identifies this field as the injection point.
- Unusual root-level process activity originating from the management web service process.
- Administrator-level configuration changes in appliance logs at unexpected times or from unexpected source addresses.

The weakness behind it

The record classes this as CWE-78 (Improper Neutralization of Special Elements used in an OS Command).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The flaw injects OS commands through a configuration field; the record says those commands execute with root privileges, which would typically involve a command interpreter on the appliance.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	An authenticated administrator's injected commands run with root privileges, escalating beyond the normal permission level the account already holds.
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	When chained with CVE-2026-116606 on ESG, an attacker with access to an internet-facing Admin UI would likely exploit the application to gain initial access without valid credentials.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Barracuda Networks Email Security Gateway (ESG), Load Balancer, Application Delivery Controller (ADC), Message Archiver (BMA), WAF Control Center (WCC), Web Application Firewall (WAF), and Web Security Gateway (WSG) contain an OS command injection vulnerability. This vulnerability could allow an authenticated administrator to inject OS commands that execute with root privileges when the crafted timezone value is subsequently processed. This vulnerability can be chained with CVE-2026-116606*

The CVE record, published by Mandiant on 2 November 2026:

> *Improper neutralization of shell metacharacters in the timezone configuration field in certain Barracuda appliance products using common Barracuda code allows an authenticated administrator to inject OS commands that execute with root privileges when the crafted timezone value is subsequently processed.*

Versions of Barracuda Networks Barracuda Email Security Gateway (ESG) the record lists as affected:

- all versions up to and including 9.4.0.27

Versions of Barracuda Networks Barracuda Load Balancer Application Delivery Controller (ADC) the record lists as affected:

- all versions up to and including 6.4.0

Versions of Barracuda Networks Barracuda Web Application Firewall (WAF) the record lists as affected:

- all versions up to and including 11.0.1

Versions of Barracuda Networks Barracuda Web Security Gateway (WSG) the record lists as affected:

- all versions up to and including 16.1.100.100

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-111560
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-111560
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say which products were targeted in the observed exploitation activity.
- The sources do not give a fixed firmware version number; only patch IDs are named for each product.
- The sources do not say whether a workaround other than restricting Admin UI access is available.
- The sources do not say whether exploitation of CVE-2026-116606, the companion bypass, has also been observed.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 13 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-111560: score 8.6, `CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	High	An administrator account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
2 November 2026	CVE record published by Mandiant.
10 November 2026	CISA added it to its list of exploited vulnerabilities.
13 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

ESG with Admin UI internet-accessible and CVE-2026-116606 not yet patched	High	By 13 November 2026
Any affected appliance with Admin UI accessible from outside the internal network	High	By 13 November 2026
Affected appliance behind a firewall; patches not yet applied	Medium	This week
Running Message Archiver or WAF Control Center (named in advisory, not in CVE record)	Medium	This week — treat as affected until confirmed otherwise
Affected appliance internal-only and patches confirmed current	None	No action needed beyond confirming patch status

Appendix 4. Definition of done

- Every Barracuda Networks Multiple Products you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-111560: https://www.cve.org/CVERecord?id=CVE-2026-111560
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: trust.barracuda.com/security/pre-authentication-authorization-bypas: https://trust.barracuda.com/security/pre-authentication-authorization-bypass-command-injection
- Reference in the CVE record: github.com: https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2026/MNDT-2026-0041.md