contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Barracuda Networks Barracuda Email Security Gateway (ESG) exploited

CVE-2026-116606 · on CISA's exploited list since 10 November 2026

Analysis Report

Anyone running Barracuda Email Security Gateway must act: CISA's deadline is 13 November 2026 — today. First, check whether the ESG Admin UI is reachable from

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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-barracuda-email-security-cve-2026-116606

The bottom line

> *Anyone running Barracuda Email Security Gateway must act: CISA's deadline is 13 November 2026 — today. First, check whether the ESG Admin UI is reachable from the internet, then apply the patch that matches your firmware version.*

At a glance

Fact	Detail
Product	Barracuda Networks Barracuda Email Security Gateway (ESG) (CVE-2026-116606)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 13 November 2026.
Chance of exploitation (EPSS)	0.11, 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 firmware 9.4.0.030 or later. The advisory names patches BNSF-40425 (for firmware 9.4.017 and above) and BNSF-40430 (for firmware below 9.4.017).
Who looks first	Any organisation running Barracuda Email Security Gateway on firmware earlier than 9.4.0.030. The record lists only ESG for this CVE; other Barracuda products are not affected by CVE-2026-116606.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Barracuda Email Security Gateway (ESG)?	Nothing to do for this CVE.	Check whether your firmware is earlier than 9.4.0.030 (next question).
Is your ESG firmware earlier than version 9.4.0.030?	Verify the applicable patch is applied; check separately for CVE-2026-111560.	Apply the appropriate patch immediately — see the steps below.
Is the ESG Admin UI accessible from the internet or an untrusted network?	Exposure is reduced, but the advisory still recommends patching.	Treat as urgent; patch immediately and restrict Admin UI access.

What it is

An unauthenticated remote attacker who can reach the ESG Admin UI can trigger the configuration-import function and load a crafted backup archive, overwriting the appliance's global configuration. The advisory says chaining this with CVE-2026-111560 can give root access to the device.

Why it matters

The flaw requires no login — only access to the Admin UI. By loading a crafted backup archive, an attacker can overwrite global configuration before credentials are checked. The advisory says chaining this with CVE-2026-111560 (command injection) can give root access to the device. Barracuda updated its advisory on 9 November 2026 to confirm exploitation at a small number of organisations. Restricting the Admin UI reduces exposure but does not remove the flaw; the advisory recommends patching regardless. Our reading is that any internet-exposed ESG Admin UI should be treated as the highest-risk scenario until patched.

What the vendor's advisory says

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

- CVE-2026-111560 is a command injection flaw affecting ESG, Load Balancer ADC, Message Archiver, WAF Control Center, Web Application Firewall, and Web Security Gateway. Separate patches are available for each product.
- ESG patches: BNSF-40425 for firmware 9.4.017 and above; BNSF-40430 for firmware below 9.4.017. The advisory says devices show the latest firmware version available.
- If automatic patching is disabled, the advisory recommends re-enabling it and applying the patch manually as soon as possible.
- Barracuda updated the advisory on 9 November 2026 to confirm exploitation at a small number of organisations and to correct the authentication field: no login is needed, only Admin UI access.

Things people will get wrong

- Restricting Admin UI access to internal networks is sufficient. The advisory says restriction reduces exposure but does not remove the flaw, and recommends applying patches regardless. Exploitation has already been observed.
- This CVE only affects ESG, so our other Barracuda devices are fine. CVE-2026-116606 affects only ESG. The advisory says the companion CVE-2026-111560 also affects Load Balancer ADC, Message Archiver, WAF Control Center, Web Application Firewall, and Web Security Gateway.

How we would triage it

This is our judgement.

Step 1: Find the ESG firmware version

- Log in to the ESG Admin UI and check the firmware version shown on the system status page; the advisory says the device shows the latest available version.
- Compare the running version against 9.4.0.030 — the record lists all versions before this as affected.

Step 2: Check whether Admin UI is internet-accessible

- Review firewall rules and confirm whether the ESG admin port is reachable from outside your internal network.
- If it is, restrict access to trusted internal addresses immediately — the advisory says this reduces exposure while patching is arranged.

Step 3: Apply the appropriate patch

- If the firmware is 9.4.017 or above, apply patch BNSF-40425. If it is below 9.4.017, apply patch BNSF-40430. The advisory says to contact Barracuda Support if assistance is needed.
- If the device is multiple firmware versions out of date, the advisory says more than one update may be required; Barracuda Support can assist.

Step 4: Confirm automatic patching is enabled

- In the ESG Admin UI, confirm that automatic patching is enabled so future security patches are applied without manual intervention.
- The advisory recommends re-enabling automatic patching if it was turned off.

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 are following up on CVE-2026-116606, a pre-authentication authorisation bypass in Barracuda Email Security Gateway (ESG). CISA requires this to be remediated by 13 November 2026. Please can you confirm: whether we run any Barracuda ESG appliances and on which firmware version; whether the ESG Admin UI is accessible from outside our internal network; and whether patches BNSF-40425 or BNSF-40430 have been applied, or firmware updated to 9.4.0.030 or later. Please provide 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 ESG global configuration — particularly import events — without a corresponding authorised administrator action may indicate the import function was triggered.
- Admin UI access logs showing connections from external or unrecognised source addresses, especially around the time of any unexplained configuration changes.
- The advisory confirmed exploitation at a small number of organisations; check for any configuration state that cannot be traced to an authorised change.

The weakness behind it

The record classes this as CWE-288 (Authentication Bypass Using an Alternate Path or Channel).

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

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	The flaw is a pre-auth bypass on a network-accessible admin UI; an unauthenticated remote attacker would typically exploit the application directly to gain initial access to the appliance.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	Successful exploitation overwrites global configuration by importing a crafted archive — this would typically be used to manipulate stored configuration to change device behaviour.
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	The advisory says chaining this bypass with CVE-2026-111560 can give root access; this escalation path would typically be used to gain elevated privileges on the device.

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) contains an authentication bypass using an alternate path or channel that could allow an unauthenticated remote attacker to invoke a configuration-import function and restore a crafted, compatible backup archive, resulting in unauthorized modification of the appliance's global configuration. This vulnerability can be chained with CVE-2026-111560.*

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

> *An authentication bypass in Barracuda Email Security Gateway versions earlier than 9.4.0.030 allows an unauthenticated remote attacker to invoke a configuration-import function and restore a crafted, compatible backup archive, resulting in unauthorized modification of the appliance's global configuration.*

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

- all versions before 9.4.0.030

The affected ranges end before 9.4.0.030. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

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-2026-116606
```

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-2026-116606
```

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 state whether cloud-hosted or SaaS ESG instances are affected, or only on-premises and virtual appliances.
- The advisory does not name the sectors or regions where exploitation was observed.
- The sources do not confirm whether automatic patch delivery has already pushed the patch to internet-connected devices.

- The record does not describe what a crafted backup archive must contain to exploit the flaw, or whether detection signatures are available.
- 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-2026-116606: score 9.3, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/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	None	No 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 Admin UI exposed to the internet, firmware below 9.4.0.030	High	Immediately — CISA deadline is 13 November 2026
ESG Admin UI restricted to internal networks, firmware below 9.4.0.030	High	Within CISA's window; restrict UI access and patch today
ESG firmware at 9.4.0.030 or later, automatic patching enabled	Medium	Confirm the applicable patch is applied this week
Other Barracuda products (ADC, WAF, etc.) but no ESG	Low	Not affected by this CVE; check CVE-2026-111560 separately
No Barracuda products in use	None	Nothing to do for this CVE

Appendix 4. Definition of done

- Every Barracuda Networks Barracuda Email Security Gateway (ESG) 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-2026-116606: https://www.cve.org/CVERecord?id=CVE-2026-116606
- 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-2026-0042.md