KILLSWITCH · ISSUE #16 · 13 NOV 2026

The Email Gateway's Admin Page Was the Way In

A pre-authentication flaw makes an admin-only flaw reachable. The only precondition is an admin page the attacker can reach.

Killswitch rating: Patch and check this week

By Emmanuel Aigbehi Walstra

The email gateway's admin page was the way in

Two Barracuda flaws, used together, could give an attacker root on the device [1].

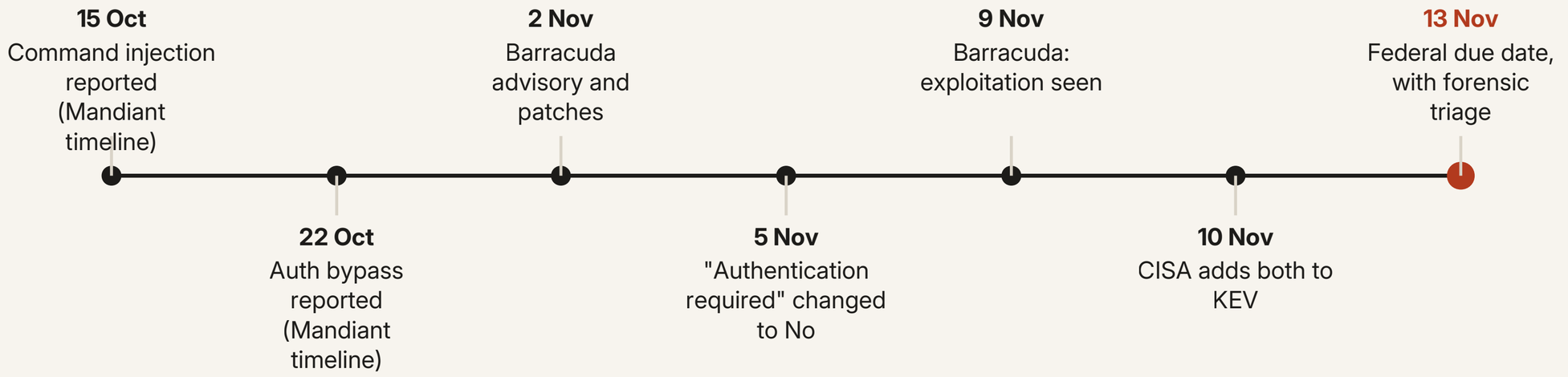
- Barracuda: exploitation seen at "a small number of organizations" (9 Nov) [1].
- CISA KEV, 10 Nov: forensic triage required; federal due date 13 Nov [4].

Both flaws need the admin page to be reachable

- "Successful exploitation requires an attacker to have access to the administrative interface" (Barracuda) [1].
- CVE-2026-116606 needs no login, only the reachable admin page [1].
- Admin page off the internet: "less exposed to this attack path" [1].

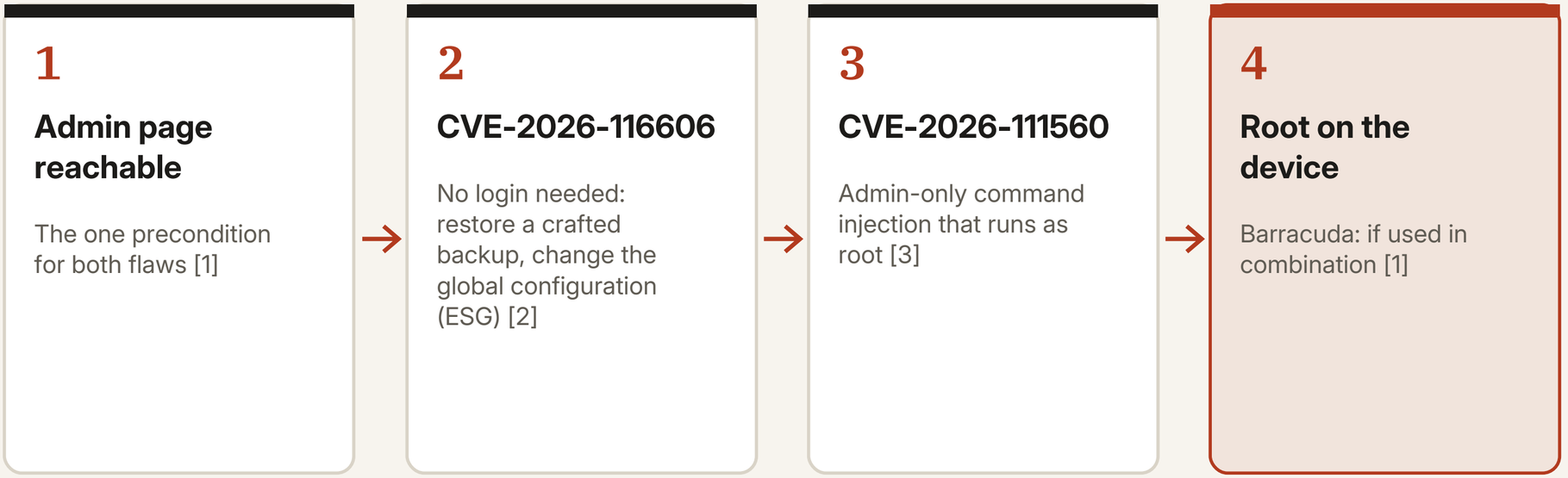
03 · TIMELINE

From report to federal deadline



Mandiant [2][3], Barracuda [1], CISA [4]. All dates 2026.

Why the admin page is the whole story



Barracuda [1], Mandiant [2][3]. Defender view only: no exploitation detail.

The line that changed on 5 November

- 2 Nov: "Authentication Required: Yes, administrative access" [1].
- 5 Nov: "No (Administrative UI Access Required)" [1].
- Triaged it on 2 or 3 November as "needs admin"? Re-read it.

06 · SCOPE

Which products are affected

1 **Email Security Gateway**

Both CVEs. The only product with the auth bypass

2 **Web Security Gateway**

CVE-2026-111560

3 **Web Application Firewall**

CVE-2026-111560

4 **WAF Control Center**

CVE-2026-111560

5 **Load Balancer ADC**

CVE-2026-111560

6 **Message Archiver**

CVE-2026-111560

Barracuda's table [1]. Patch IDs and firmware are on the vendor page; check each device's own firmware view.

Patch, then confirm on the device

- Check each device runs the latest firmware with all patches [1].
- Several versions behind: more than one update may be needed [1].
- Automatic patching off? Turn it back on [1].
- Take the fix from Barracuda's table, not a copied version number [1][2][3].

CISA's forensic triage, in six steps

1. **Scope**
   Which devices, which interfaces, since when
2. **Preserve and collect evidence**
   Volatile data first; patching may destroy artifacts
3. **Patch and stabilise**
   Apply the critical patches
4. **Contain**
   Isolate in-scope systems
5. **Analyse**
   Unauthorised access, persistence, data staging
6. **Decide**
   Report: no evidence, suspected, or confirmed

CISA BOD 26-04 implementation guidance [6]. Collect evidence before patching where you can [6].

Four controls for every appliance admin page

1 **Admin page off the internet**

Trusted internal network or VPN only

2 **Automatic patching on**

And check the firmware is current

3 **Investigate, not only patch**

Check config changes and admin activity

4 **Inventory admin interfaces**

Every appliance, every reachable port

Barracuda's guidance [1] plus Killswitch additions (inventory, evidence).

Where this lives in your frameworks

Prevent	A.8.20, A.8.22, A.8.9 · NIS2 21(2)(e) · Evidence: admin-interface exposure scan
Patch	A.8.8 · NIS2 21(2)(e) · Evidence: firmware and patch record per device
Respond	A.5.25, A.5.26, A.5.28 · NIS2 21(2)(b) · Evidence: triage report
Know	A.5.9 · NIS2 21(2)(i) · Evidence: appliance inventory

Killswitch's own mapping. Check ISO titles against your licensed copy.

ISO/IEC 27001:2022 [9] · NIS2 Art. 21(2) [8]. Killswitch mapping.

What we don't know yet

- Victims, attacker and post-access activity: not disclosed [1].
- Whether every case used both flaws: not stated [1][4].
- No indicators of compromise published in the advisory [1].
- Ransomware use: "Unknown" (CISA) [4].

This week

- List every affected Barracuda device, including MSP-run ones.
- Check from outside whether admin pages are reachable; restrict them.
- Collect logs and config, patch, confirm firmware.
- Turn automatic patching back on.
- Run and record a triage for exposed devices.

Sources

[1] Barracuda: Pre-Authentication Authorization Bypass and Command Injection Vulnerabilities in Certain Barracuda Products (2 Nov 2026, updated 5 and 9 Nov)
[2] Mandiant: MNDT-2026-0042, CVE-2026-116606, Barracuda ESG authentication bypass (2 Nov 2026)
[3] Mandiant: MNDT-2026-0041, CVE-2026-111560, Barracuda command injection (2 Nov 2026)
[4] CISA: Known Exploited Vulnerabilities Catalog (CVE-2026-116606 and CVE-2026-111560 added 10 Nov 2026)
[5] CISA: BOD 26-04, Prioritizing Security Updates Based on Risk
[6] CISA: BOD 26-04 Implementation Guidance (Forensic Triage Steps)
[7] CVE record: CVE-2026-116606 (CNA: Mandiant)
[8] NIS2 Directive (EU) 2022/2555, Article 21 (EUR-Lex)
[9] ISO/IEC 27001:2022 Information security management systems
[10] NVD: CVE-2026-116606 and CVE-2026-111560 (analysed 12 Nov 2026)

Facts are from Barracuda's advisory (updated 9 November), Mandiant's advisories, the CVE record and CISA's KEV catalog and BOD 26-04 guidance, as published by 10 Nov 2026. Barracuda has not named the affected organisations or the attacker. The controls and the framework mapping are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Know which admin pages face the internet, and prove they are closed

GRCOMPLIANCE

Keep an inventory of internet-facing assets and their admin interfaces, track patches and forensic checks as evidence, and map controls to ISO 27001 and NIS2.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.