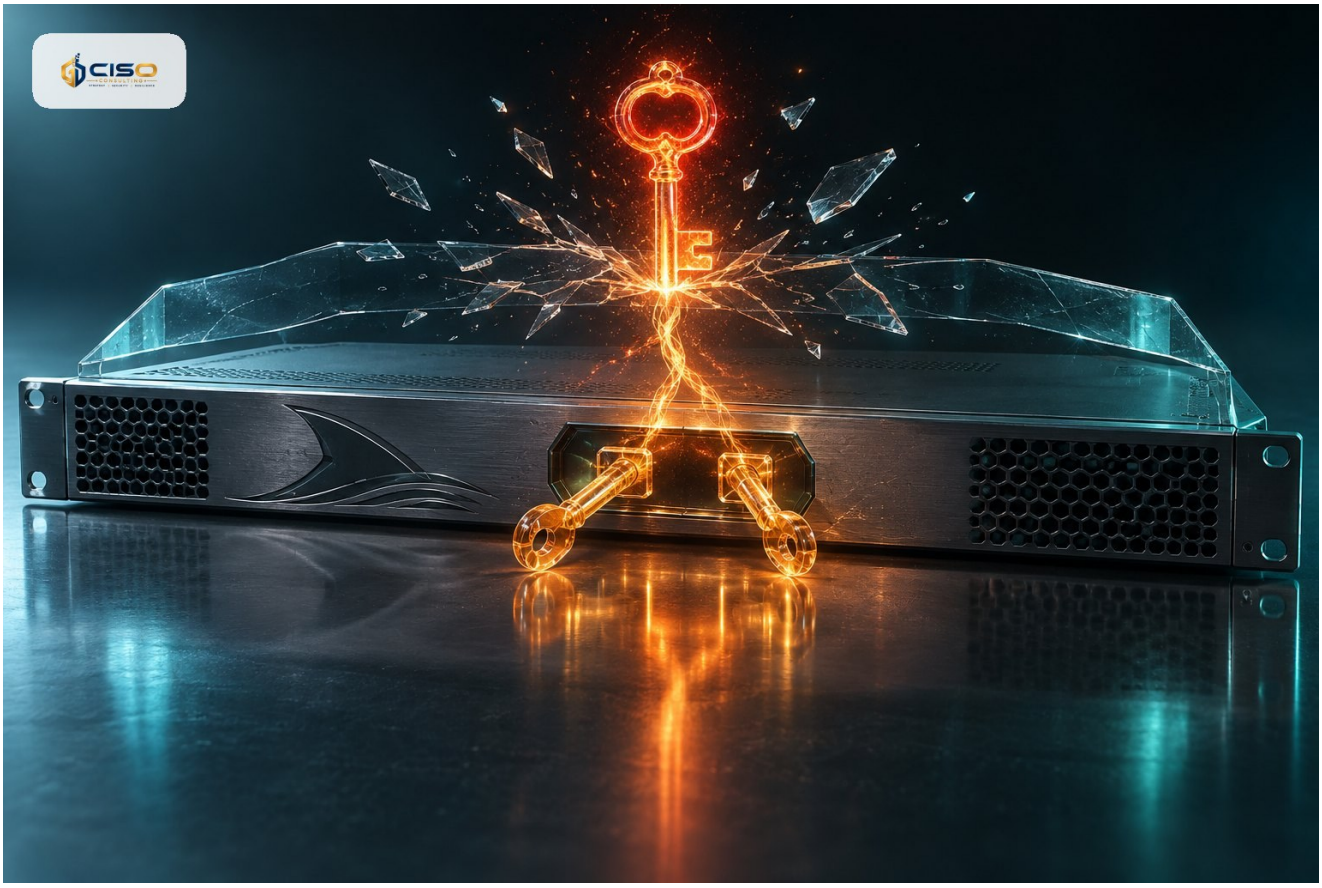
Barracuda patches two flaws that can lead to root access on its appliances



Barracuda has released patches for CVE-2026-116606 and CVE-2026-111560, which together could let an attacker with administrative interface access gain root on affected appliances. Customers are urged to update firmware and restrict admin access.

- CVE-2026-116606 is a critical authentication weakness in Email Security Gateway that allows changes to the appliance's global configuration.
- CVE-2026-111560 lets an attacker with admin permissions inject OS commands that run as root.
- Exploitation requires access to the administrative interface; combined, the flaws could bypass authorization and give root access.
- Affected products also include Load Balancer ADC, Message Archiver, WAF Control Center, Web Application Firewall and Web Security Gateway.

> - Barracuda ESG appliances were targeted in earlier zero-day campaigns in 2023.

Barracuda Networks has told customers to apply patches for two vulnerabilities that can allow commands to run with root privileges on its appliances.

What the flaws do

The first, **CVE-2026-116606**, is rated critical. It stems from an authentication weakness in the Email Security Gateway (ESG) that an attacker can use to modify the appliance's global configuration. The second, **CVE-2026-111560**, allows an attacker who already holds admin permissions to inject operating system commands that execute as root.

Barracuda states that exploitation requires access to the administrative interface of the targeted product. If the two flaws are used together, an attacker could bypass authorization controls and obtain root access to the device.

Affected products and fixes

Besides ESG, the vendor's list covers Load Balancer ADC, Message Archiver (BMA), WAF Control Center (WCC), Web Application Firewall (WAF) and Web Security Gateway (WSG). Patches are identified by references such as BNSF-40425 for ESG 9.4.017 and later and BNSF-40430 for earlier versions. Barracuda asks customers to review the remediation guidance, run the latest firmware and apply all security patches. It also advises network access controls that limit administrative access to trusted internal networks.

Context

ESG appliances have been attacked before. Barracuda patched CVE-2023-7102 after the UNC4841 group exploited it as a zero-day, and the same group abused CVE-2023-2868 in espionage attacks that, per Mandiant, hit government agencies heavily. The source does not report exploitation of the new flaws.

What to do now

1. Inventory all Barracuda ESG, ADC, BMA, WCC, WAF and WSG appliances and confirm their firmware versions.
2. Apply the vendor patches listed for each affected product, prioritising Email Security Gateway.
3. Restrict administrative interfaces to trusted internal networks and block access from the internet or general user segments.
4. Review admin accounts and recent configuration changes on these appliances for anything unexpected.
5. Record the patching in your vulnerability management process in line with NCA ECC and SAMA CSF requirements.