AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-116606

Konfigurationsübernahme ohne Anmeldung im Barracuda Email Security Gateway.

Über einen alternativen Zugangsweg kann ein Angreifer ohne Anmeldung die Import-Funktion des Barracuda Email Security Gateway aufrufen und ein präpariertes Backup einspielen – damit überschreibt er die globale Konfiguration des Mail-Gateways. Kombiniert mit der Command Injection CVE-2026-111560 führt das bis zu Root-Rechten. Barracuda bestätigt Angriffe auf einzelne Organisationen; Patches sind verfügbar.

> **Geschäftsrisiko:** Übernahme des zentralen Mail-Gateways: Umleitung, Mitlesen oder Manipulation der gesamten E-Mail-Kommunikation, Abschalten von Schutzfiltern und ein dauerhafter Brückenkopf im Netz – ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist wahrscheinlich.

9,3 / 10

KRITISCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`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` – aus dem Netz, ohne Rechte, ohne Zutun, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Vergeben von Mandiant als CNA; Barracuda nennt denselben Wert, stuft verbal aber nur „High“ ein.

IN CISA KEV SEIT	BETROFFEN	HANDLUNGSBEDARF
10. November 2026	ESG-Firmware vor 9.4.0.030	Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,3 · KRITISCH
CVSS 4.0 (Mandiant)

Auth-Bypass
Backup-Import ohne Anmeldung · CWE-288

Aktiv
ausgenutzt · CISA KEV · Frist 13.11.2026

Patch da
BNSF-40425 / BNSF-40430

Die Ursache: Das ESG prüft die Berechtigung nicht auf allen Wegen, über die seine Verwaltungsfunktionen erreichbar sind (**CWE-288, Authentication Bypass über einen alternativen Pfad**). Ein Angreifer, der die Administrationsoberfläche erreicht, kann ohne Anmeldung den **Konfigurations-Import** auslösen und ein präpariertes, kompatibles Backup zurückspielen. Zusammen mit **CVE-2026-111560** (Command Injection im Zeitzonen-Feld, Root-Rechte) entsteht eine Kette bis zur vollständigen Geräteübernahme.

ANGRIFFSKETTE

01	02	03	04
Admin-UI erreichbar – Verwaltungsoberfläche aus dem Netz ansprechbar	**Backup einspielen** – Import ohne Anmeldung (CVE-2026-116606)	**Root-Befehle** – Zeitzonen-Feld als Hebel (CVE-2026-111560)	**Mail-Gateway übernommen** – Mails umleiten, Filter aus

Betroffenheit & Fixversionen

ESG-Firmware	Verwundbar bis	Fixversion (Ziel)
ESG ab 9.4.017	vor 9.4.0.030	Patch BNSF-40425
ESG vor 9.4.017	alle	Patch BNSF-40430
Zielstand Firmware	< 9.4.0.030	9.4.0.030 oder neuer

Betroffen ist laut CVE-Eintrag (Mandiant als CNA) jede ESG-Firmware **vor 9.4.0.030**. Barracuda verteilt die Patches automatisch – wer Auto-Patching abgeschaltet hat, muss manuell nachziehen. Die Kettenlücke CVE-2026-111560 betrifft zusätzlich Load Balancer ADC, WAF, WAF Control Center, Web Security Gateway und Message Archiver.

Regulatorischer Hinweis: Ein bestätigter Zugriff auf das Mail-Gateway betrifft regelmäßig personenbezogene Daten und kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

02.11.2026
Barracuda-Advisory und Patches

05.11.2026
Korrektur: keine Anmeldung nötig

09.11.2026
Barracuda bestätigt Angriffe

10.11.2026
CISA KEV · Frist 13.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Admin-UI abschotten	Patch und 9.4.0.030	Konfiguration prüfen

01 Admin-Oberfläche abschotten

Prüfen, ob die Administrationsoberfläche des ESG aus dem Internet oder aus Fremdnetzen erreichbar ist, und den Zugriff auf vertrauenswürdige interne Verwaltungsnetze beschränken – so empfiehlt es auch Barracuda.

02 Patchstand verifizieren

Firmware ermitteln: ab `9.4.017` muss `BNSF-40425` installiert sein, darunter `BNSF-40430`. Zielstand ist `9.4.0.030` oder neuer; bei veralteter Firmware ggf. mehrere Update-Schritte.

03 Automatische Patches einschalten

Ist Auto-Patching deaktiviert, Patch manuell einspielen und die Automatik wieder aktivieren. Weitere Barracuda-Geräte (WAF, ADC, WSG, BMA, WCC) wegen `CVE-2026-111560` gleich mitprüfen.

04 Kompromittierung ausschließen

Globale Konfiguration mit einem bekannten Sollstand vergleichen: Weiterleitungen, Relay-Ziele, Administratorkonten, Filter- und Zeitzonen-Einstellungen. Bei Abweichungen Gerät als kompromittiert behandeln und Barracuda-Support einbinden.

Kompromittierungs-Indikatoren (IoCs)

HERSTELLER-IOCS

Von Barracuda
nicht veröffentlicht
(Stand 11.11.2026)

PRÜFANSATZ KONFIGURATION

Unerwarteter Backup-Import
neue Weiterleitungen / Relays
geänderte Zeitzonen-Werte

PRÜFANSATZ ZUGRIFF

Admin-UI-Aufrufe von
unbekannten Quellen
neue Admin-Konten

Zur Einordnung: Das sind allgemeine Prüfansätze von Argos, abgeleitet aus der Fehlerbeschreibung, keine bestätigten Indikatoren. Angreifer und Umfang der Ausnutzung sind nicht veröffentlicht. Ein unauffälliges Ergebnis schließt einen Zugriff daher nicht aus.

Wichtig: Der Patch schließt die Lücke, setzt aber eine bereits eingespielte Fremdkonfiguration nicht zurück. Wer das Mail-Gateway kontrolliert, sieht die gesamte E-Mail-Kommunikation – deshalb gehört der Konfigurationsabgleich zwingend mit auf den Prüfplan.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Ein Konfigurations-Import oder Admin-Zugriff auf das ESG von unbekannter Quelle fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare ESG-Admin-Oberflächen über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre Barracuda ESG-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Patchstand aller Barracuda-Geräte bis 13.11. bestätigen lassen.
- Admin-Oberflächen nur aus internen Verwaltungsnetzen zulassen.
- Konfigurationsabgleich des Mail-Gateways anordnen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-116606 und dem Barracuda ESG-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Barracuda Advisory (02.11., Update 09.11.2026) · CVE-Record (Mandiant, MNDT-2026-0042) · NVD · CISA KEV (10.11.2026, Frist 13.11.2026). Stand 11.11.2026.