Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0465

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Barracuda Email Security Gateway

Publicatiedatum: 04-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Barracuda heeft kwetsbaarheden verholpen in Barracuda Email Security Gateway.

Duiding

Barracuda heeft twee kwetsbaarheden vastgesteld in verschillende Barracuda-producten: een kwetsbaarheid voor het omzeilen van autorisatiecontroles (CVE-2026-116606) en een kwetsbaarheid voor command injection (CVE-2026-111560).

De eerste kwetsbaarheid betreft een pre-authentication authorization bypass in Barracuda Email Security Gateway (ESG). De tweede kwetsbaarheid betreft command injection en treft naast ESG ook de Load Balancer Application Delivery Controller (ADC), Message Archiver (BMA), WAF Control Center (WCC), Web Application Firewall (WAF) en Web Security Gateway (WSG).

Volgens Barracuda is voor succesvolle exploitatie toegang tot de administratieve interface van een kwetsbaar product vereist. Wanneer beide kwetsbaarheden in combinatie worden misbruikt, kan een aanvaller autorisatiecontroles omzeilen en roottoegang tot het apparaat verkrijgen.

Oplossingen

Barracuda heeft beveiligingspatches beschikbaar gesteld en adviseert klanten hun systemen bij te werken naar de nieuwste firmwareversie en alle beschikbare beveiligingsupdates te installeren. Daarnaast adviseert het bedrijf administratieve interfaces uitsluitend toegankelijk te maken vanuit vertrouwde interne netwerken en de toegang met passende netwerkbeveiligingsmaatregelen te beperken.

Referenties

- https://trust.barracuda.com/security/pre-authentication-authorization-bypass-command-injection

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-116606	9.3 CRITICAL
CVE-2026-111560	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

Barracuda
Web Security Gateway

Barracuda Networks
Barracuda Load Balancer Application Delivery Controller (ADC)
Barracuda WAF Control Center (WCC)
Barracuda Web Application Firewall (WAF)
Email Security Gateway
Message Archiver

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.