National Cyber Security Centre

2306010129-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert (Update)

Critical vulnerability within Barracuda Email Security Gateway Appliance (ESG) version 1.1

Friday 9th June, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Version history

Date	Version number
1 June 2023	Version 1.0
8 June 2023	Version 1.1

Description

Barracuda Networks has identified a remote command injection vulnerability (CVE-2023-2868) in the Barracuda ESG product. The vulnerability stems from incomplete input validation of .tar files, allowing an attacker to remotely execute a system command with the privileges of the ESG product. Barracuda Networks have reported that this vulnerability has been exploited since at least October 2022.

Barracuda have advised that all impacted ESG appliances must be immediately replaced regardless of patch version level. Details are available here: https://www.barracuda.com/company/legal/esg-vulnerability

Products Affected

This vulnerability affects the following:

- Barracuda ESG Appliance - versions 5.1.3.001 - 9.2.0.006

Impact

Exploitation of CVE-2023-2868 could allow an attacker to execute remote commands with the privileges of the ESG appliance.

Barracuda Networks have evidence of activity exploiting this vulnerability starting from October 2022 against a limited number of customers. These affected customers have been notified by Barracuda Networks. In these exploitation attempts, persistent malware was deployed with the abilities to upload/download files, proxy/tunnel traffic, and monitor SMTP traffic on the device.

Barracuda Network incident response teams have identified malware, backdoors, and other custom utilities that were used to move laterally within targeted environments and exfiltrate data. Further information can be found in the following link: https://www.barracuda.com/company/legal/esg-vulnerability

Recommendations

The NCSC advises that organisations replace impacted Barracuda ESG appliances as soon as possible.

Any impacted Barracuda customers who have not yet replaced their appliances are advised to contact Barracuda support at support@barracuda.com.

Full details are available here: https://www.barracuda.com/company/legal/esg-vulnerability

The NCSC also advises that organisations with ESG appliances perform a compromise assessment using the IOC's found in the links below.

- https://www.barracuda.com/company/legal/esg-vulnerability
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie