UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0324

BARRACUDA EMAIL SECURITY RCE FLAW

DATE ISSUED: 7th June 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Barracuda Networks has released a security patch for a zero-day vulnerability in its Email Security Gateway (ESG) appliance. It could allow an unauthenticated, remote attacker to perform remote code execution on the target system.

BREAKDOWN

A critical vulnerability is discovered in Barracuda Email Security Gateway (ESG) appliance, which could allow an unauthenticated, remote attacker to send a specially crafted archive to the appliance and execute arbitrary Perl commands on the target system. The high-severity vulnerability is tracked as CVE-2023-2869, with a CVSS score of 9.8. This vulnerability results from improper sanitisation of the processing of .tar files (tape archives). The incomplete input validation of a user-supplied .tar file could allow an attacker to format these file names in a way that will result in remotely executing a system command through Perl's qx operator with the privileges of the ESG. The affected versions of ESG are 5.1.3 - 9.2. The Cybersecurity & Infrastructure Security Agency (CISA) has also added the vulnerability to its Known Exploited Vulnerabilities Catalog based on evidence of active exploitation.

REMEDIATION STEPS

- Update the ESG appliance with the latest security patches recommended by Barracuda.
- Update all credentials related to the affected appliances.
- Investigate the network logs to identify the Indicator of Compromise (IOC) shared by Barracuda. Refer to IOC here https://www.barracuda.com/company/legal/esg-vulnerability#:~:text=the%20section%20below.-,Endpoint%20IOCs,-Table%204%20lists.
- Block unnecessary file types attempting to enter the enterprise's email gateway.
- Use DNS filtering services on all enterprise assets to block access to known malicious domains.

REFERENCES & RESOURCES

CIS Advisories	https://www.cisecurity.org/advisory/a-vulnerability-in-barracuda-email-security-gateway-could-allow-for-remote-command-injection_2023-054
Malwarebytes	https://www.malwarebytes.com/blog/news/2023/05/barracuda-networks-patches-zero-day-vulnerability-in-email-security-gateway
Bleeping Computer	https://www.bleepingcomputer.com/news/security/barracuda-warns-of-email-gateways-breached-via-zero-day-flaw/