June 2, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Barracuda Email Security Gateway Appliance (ESG) Vulnerability. The vulnerability affects versions 5.1.3.001-9.2.0.006.

Technical Details

Barracuda Networks identified a remote command injection vulnerability (CVE-2023-2868) present in the Barracuda Email Security Gateway (appliance form factor only) versions 5.1.3.001-9.2.0.006. The vulnerability stemmed from incomplete input validation of user supplied .tar files as it pertains to the names of the files contained within the archive. Consequently, a remote attacker could format file names in a particular manner that would result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product.

Timeline

- On May 18, 2023, Barracuda was alerted to anomalous traffic originating from Barracuda Email Security Gateway (ESG) appliances.
- On May 18, 2023, Barracuda engaged Mandiant, leading global cyber security experts, to assist in the investigation.
- On May 19, 2023, Barracuda identified a vulnerability (CVE-2023-28681) in our Email Security Gateway appliance (ESG).
- On May 20, 2023, a security patch to remediate the vulnerability was applied to all ESG appliances worldwide.
- On May 21, 2023, a script was deployed to all impacted appliances to contain the incident and counter unauthorized access methods.
- A series of security patches are being deployed to all appliances in furtherance of our containment strategy.

Barracuda's investigation to date has determined that a third party utilized the technique described above to gain unauthorized access to a subset of ESG appliances. The references below, in addition to the attached spreadsheet provide additional details for security and technical teams to consider in the mitigation of these exposed vulnerabilities.

SALTWATER is a trojanized module for the Barracuda SMTP daemon (bsmtpd) that contains backdoor functionality. The capabilities of SALTWATER include the ability to upload or download arbitrary files, execute commands, as well as proxy and tunneling capabilities.

SEASPY is an x64 ELF persistence backdoor that poses as a legitimate Barracuda Networks service and establishes itself as a PCAP filter, specifically monitoring traffic on port 25 (SMTP) and port 587. SEASPY contains backdoor functionality that is activated by a "magic packet".

Mandiant analysis has identified code overlap between SEASPY and cd00r, a publicly available backdoor.

SEASIDE is a Lua based module for the Barracuda SMTP daemon (bsmtpd) that monitors SMTP HELO/EHLO commands to receive a command and control (C2) IP address and port which it passes as arguments to an external binary that establishes a reverse shell.

Please refer to the Barracuda advisory link below for indicators of Compromise (IoCs).

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software patch has been deployed to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-2868
- Barracuda Email Security Gateway Appliance (ESG) Vulnerability