FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

23 August 2023

FLASH Number

AC-000172-TT

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:CLEAR**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI San Francisco immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email: sf-barracudacve@fbi.gov

Suspected PRC Cyber Actors Continue to Globally Exploit Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868)

Summary

As a part of the FBI investigation into the exploitation of CVE-2023-2868, a zero-day vulnerability in Barracuda Network's Email Security Gateway (ESG) appliances, the FBI has independently verified that all exploited ESG appliances, even those with patches pushed out by Barracuda, remain at risk for continued computer network compromise from suspected PRC cyber actors exploiting this vulnerability. For more details regarding malware found to date related to this exploit and learn more about Barracuda backdoors, please visit CISA Releases Malware Analysis Reports on Barracuda Backdoors. The cyber actors utilized this vulnerability to insert malicious payloads onto the ESG appliance with a variety of capabilities that enabled persistent access, email scanning, credential harvesting, and data exfiltration. The FBI strongly advises all affected ESG appliances be isolated and replaced immediately, and all networks scanned for connections to the provided list of indicators of compromise immediately. https://go.fbinet.fbi/news/Pages/Bringing-Private-Sector-to-the-Fight-Against-Cyber-Adversaries.aspx

Technical Details

CVE-2023-2868 is a remote command injection vulnerability that allows for unauthorized execution of system commands with administrator privileges on the ESG product. This vulnerability is present in the Barracuda ESG (appliance form factor only) versions 5.1.3.001-9.2.0.006, and relates to a process that occurs when the appliance screens email attachments. The vulnerability allows cyber actors to format TAR file attachments in a particular manner and send them to an email address affiliated with a domain that has an ESG appliance connected to it. The malicious file's formatting, when scanned, results in a command injection into the ESG that leads to system commands being executed with the privileges of the ESG. As the vulnerability exists in the scanning process, emails only need to be received by the ESG to trigger the vulnerability.

The earliest evidence of exploitation of Barracuda ESG appliances was observed in October 2022. Initially, suspected PRC cyber actors sent emails to victims containing TAR file attachments designed to exploit the vulnerability. In the earliest emails, attached files had a ".tar" extension in the filename, while later emails included different file extensions such as ".jpg" or ".dat". The malicious email attachments contained files that initiated a connection to a domain or IP address controlled by the cyber actors and established a reverse shell at that domain or IP address, allowing the actors to execute further commands on the ESG device.

After the suspected PRC cyber actors compromised the device, they were observed dropping various malicious payloads into the vulnerable machines and aggressively targeted specific data for exfiltration. In some cases, the actors used initial access to the ESG appliance as an entry point to the rest of the victim's network or sent emails to other victim appliances. The cyber actors used additional tools to maintain long-term, persistent access to the ESG appliances.

Based on the FBI's investigation to date, the cyber actors exploited this vulnerability in a significant number of ESG appliances and injected multiple malicious payloads that enabled persistent access, email scanning, credential harvesting, and data exfiltration. In many cases, the cyber actors obfuscated their actions with counter-forensic techniques, making detection of compromise difficult through only scanning the appliance itself for indicators of compromise. As a result, it is imperative that networks scan various network logs for connections to any of the listed indicators.

Indicators

Domains			
bestfindthetruth[.]com	goldenunder[.]com	singamofing[.]com	togetheroffway[.]com
gesturefavour[.]com	singnode[.]com	fessionalwork[.]com	

IP Addresses			
101.229.146.218	23.224.42.29	139.84.227.9	107.173.62.158
103.146.179.101	23.224.78.130	155.94.160.72	137.175.19.25
103.27.108.62	23.224.78.131	182.239.114.135	137.175.28.251
103.77.192.13	23.224.78.132	182.239.114.254	137.175.30.36
103.77.192.88	23.224.78.133	192.74.226.142	137.175.30.86
103.93.78.142	23.224.78.134	192.74.254.229	137.175.51.147
104.156.229.226	37.9.35.217	198.2.254.219	137.175.53.17
104.223.20.222	38.54.113.205	198.2.254.220	137.175.53.170
107.148.149.156	38.54.1.82	198.2.254.221	137.175.53.218
107.148.219.227	38.60.254.165	198.2.254.222	137.175.60.252
107.148.219.53	45.63.76.67	198.2.254.223	137.175.60.253
107.148.219.54	52.23.241.105	199.247.23.80	137.175.78.66
107.148.219.55	64.176.4.234	213.156.153.34	216.238.112.82
107.148.223.196	64.176.7.59	195.234.82.132	**54.197.109.223***
185.243.41.209*	**155.94.160.95***	**45.154.253.153***	**45.154.253.154***
173.201.39.85*			

Note: Bolded IPs are previously unidentified IOCs discovered through an FBI investigation.

Information Requested:

If a compromise is detected, please contact the FBI at **sf-barracudacve@fbi.gov** and provide the following:

1. Indicators of compromise related to the activity to include:

- Copies of virtual/physical images (memory and/or appliance images)
- Log files
- Malware samples
- Date and timeframes of malicious activity
- Information regarding lateral movement or exfiltration

2. Description of malicious activity observed

3. If a third-party remediation firm was engaged, please provide the firm's report and artifacts.

Recommended Mitigations:

Through an investigation of the Barracuda ESG appliance compromise, the FBI discovered additional indicators of compromise as well as independently verified many of the indicators of compromise in the public domain. Barracuda customers should remove all ESG appliances

immediately. The patches released by Barracuda in response to this CVE were ineffective. The FBI continues to observe active intrusions and considers all affected Barracuda ESG appliances to be compromised and vulnerable to this exploit. In addition, customers should further investigate for any further compromise by conducting scans for outgoing connections using the list of indicators provided as the malicious cyber actors have demonstrated the ability to compromise email accounts and computer networks, as well as maintain persistence in victim networks for continued future operations and data exfiltration. Customers who used enterprise privileged credentials for management of their Barracuda appliances (such as Active Directory Domain Admin) should immediately take incident investigation steps to verify the use and behavior of any credentials used on their devices. Investigation steps may include:

- Review email logs to identify the initial point of exposure;
- Revoke and rotate all domain-based and local credentials that were on the ESG at the time of compromise;
- Revoke and reissue all certificates that were on the ESG at the time of compromise
- Monitor entire network for the use of credentials that were on the ESG at the time of compromise;
- Review network logs for signs of data exfiltration and lateral movement;
- Capture forensic image of the appliance and conduct a forensic analysis.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to **sf-barracudacve@fbi.gov** or their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:CLEAR.** The information in this product may be shared with peers and partner organizations within your sector or community but not via publically accessible channels.