Barracuda ESG: CVE-2023-2868 Hardening Recommendations

V1.1 – JUNE 30, 2023

MANDIANT PROPRIETARY

Change Log

Version / Date	Notes
1.0: June 15, 2023	Initial Public Release
1.1: June 30, 2023	Corrected Secure LDAP link on Page 7

Contents

Barracuda ESG: CVE-2023-2868 Architecture Hardening Recommendations

CVE-2023-2868 Overview

On May 19, 2023, Barracuda Networks identified a remote command injection vulnerability (CVE-2023-2868) present in Barracuda Email Security Gateway (ESG) appliances (versions 5.1.3.001-9.2.0.006). The vulnerability stemmed from incomplete input validation of user supplied .tar files. Consequently, a remote attacker could format file names in a particular manner, resulting in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product.

Barracuda's investigation to date has determined that a threat actor utilized the technique described above to gain unauthorized access to a subset of ESG appliances.

On June 06, 2023, Barracuda reiterated its guidance that impacted customers replace compromised ESG appliances immediately, regardless of patch version level. Customers are advised to contact Barracuda support for assistance (support@barracuda.com).

For a listing of specific timelines and observed Indicators of Compromise (IOCs) related to CVE-2023-2868, reference:

https://www.barracuda.com/company/legal/esg-vulnerability

If the organization is not able to immediately discontinue the use of and replace the compromised ESG appliance, Mandiant recommends creating a separate VLAN restricting egress communication to segment the appliance from the rest of the organization’s environment until it is replaced with a new appliance.

Document Scope

This document provides architectural hardening recommendations to mitigate the potential impact of a compromised ESG appliance being leveraged for lateral movement or expanded access within an organization. While some of the recommendations are specific to Barracuda ESG appliances, as a best practice, many of the architectural recommendations should be considered for properly securing an organization's infrastructure.

Barracuda Recommendations

The following document contains Barracuda’s recommendations for securing the deployment of Barracuda ESG.

https://campus.barracuda.com/product/emailsecuritygateway/doc/9011839/securing-the-barracuda-email-security-gateway/

Barracuda ESG Hardening

Network Communication Restrictions

Hardening Goals: Restrict the scope of permitted communications to/from Barracuda ESG appliances.

Internal Communications Restrictions

For Barracuda ESG appliances that have internally routable IP addresses assigned, the appliance interface(s) should be configured within a designated VLAN, which has restricted ingress and egress communications. Specifically, the appliance(s) should be denied from communicating with both internal and external endpoints and services, and only permitted allow-list communications to defined applications and services.

At a minimum, the following common protocols and ports should be blocked from being accessible from the ESG appliance(s), as these could be leveraged for lateral movement purposes:

- SMB (TCP/445)
- RDP (TCP/3389)
- WMI (TCP/135 & TCP/1024 - TCP/65536)
- WINRM (TCP/5985 & TCP/5986)
- SSH (TCP/22)
- HTTP / HTTPs (TCP/80 & TCP/443) *

  **east / west traffic only – as outbound HTTP/HTTPs traffic is required for proper functioning of the ESG (detailed below)*

External Communications Restrictions

To reduce the exposure and potential attack surface for **inbound traffic**, Barracuda ESG appliances should be placed behind a Layer 7 firewall or network filtering appliance, with only the necessary ports and services being externally accessible based upon the intended configuration (e.g., TCP/25 (SMTP) via port forwarding for receiving email).

For Barracuda ESG interfaces that can communicate with external addresses (**outbound traffic**), egress communications should follow a **deny-list approach** using a Layer 7 firewall or network filtering appliance, which only permits application-related services for the scope of egress communications. This approach can prevent against potential backdoors or reverse shells from establishing egress connectivity to command and control infrastructure.

For additional Information related to these configurations, reference:

https://campus.barracuda.com/product/emailsecuritygateway/doc/3866640/deployment-behind-the-corporate-firewall

https://campus.barracuda.com/product/emailsecuritygateway/doc/3866676/how-to-route-outbound-mail-from-the-barracuda-email-security-gateway/

https://campus.barracuda.com/product/campus/doc/89096320/required-outbound-connections-for-barracuda-networks-appliances

Administrative Access

Administrative access to the Barracuda ESG should be permitted via an allow-list only approach. The associated management port should not be Internet-accessible - and should only be reachable from pre-defined IP addresses. This can be configured via the `BASIC > Administration` ESG UI page (`Administrator/IP Range` settings).

ESG appliances can also allow for remote administration and configuration using an API. API access to an ESG is secured using a password. **The API password should be regularly and proactively rotated.**

To limit access to an ESG appliance using an API, the `Allowed SNMP and API IP/Range` setting within the `BASIC > Administration` ESG UI page can be leveraged.

For additional Information related to the API configuration and usage options, reference:

> https://campus.barracuda.com/product/emailsecuritygateway/doc/76284988/barracuda-email-security-gateway-api-guide

Patching and Updates

Hardening Goals: Ensure that appliances are running the latest software and firmware updates

In addition to receiving updates related to product vulnerabilities, Barracuda recommends that Energize Updates are enabled, Firmware Patches are set to Automatically Apply, and that all firmware updates are downloaded and applied.

For additional information related to this configuration, reference:

> https://campus.barracuda.com/product/emailsecuritygateway/doc/31393709/step-4-product-activation-and-firmware-update/

Note: Firmware updates should be applied during scheduled maintenance windows as the updates will require a reboot of the ESG appliance.

If ESG is being leveraged within a Microsoft Exchange environment and the Barracuda Exchange Antivirus Agent is installed on mailbox servers, Mandiant recommends that virus definitions have the **Automatic Update** attribute set to **On**.

For additional information related to this configuration, reference:

> https://campus.barracuda.com/product/emailsecuritygateway/doc/3866708/how-to-get-and-configure-the-barracuda-exchange-antivirus-agent-6-0-x

ESG Credential Rotation and Segmentation

Hardening Goal: Rotate and segment credentials associated with administrative or integrated access for Barracuda ESG appliances.

Credential Rotation

Mandiant and Barracuda recommend the practice of not reusing local passwords across systems, such as the admin and API password. Upon receiving a replacement ESG appliance, Barracuda recommends using new passwords for each account. This includes rotating the credentials for identities (accounts) and services (e.g., API access password, certificates).

Additionally, ESG appliances support the ability for accounts to be authenticated using either LDAP, Active Directory, POP, or RADIUS. For any accounts that are configured in this manner, the associated passwords should be proactively rotated within the respective identity provider platform. Mandiant also recommends rotating any application credentials connected to the ESG appliance, such as Barracuda Cloud Control, FTP Server, SMB, and any private TLS certificates.

If Secure LDAP was configured, the associated certificates should also be rotated. For additional information related to this configuration, reference:

> https://campus.barracuda.com/product/essentials/doc/3211273/how-to-configure-user-authentication-using-ldap

Credential Segmentation

When integrating Barracuda ESG appliances with existing identity stores (e.g., LDAP, Active Directory) or services (e.g., email), dedicated service accounts should be leveraged for creating the integration bind. Creating dedicated accounts for each service integration can minimize potential service impacts of a password rotation for a defined account. Additionally, the service accounts should be configured based upon the concept of least-privilege, with authentication and usage restrictions enforced within the identity provider.

For further details, reference:

> https://campus.barracuda.com/product/campus/doc/91980494/security-for-integrating-with-other-systems-best-practices

Using Active Directory as an example, to minimize the potential for lateral movement and privilege escalation, any "service" accounts which are created for integrating Barracuda ESG appliances can likely have the following user-rights assignment restrictions enforced within a group policy object (GPO):

```
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User
Rights Assignment
```

- Deny log on locally (“SeDenyInteractiveLogonRight”)
- Deny log on through Terminal Services (“SeDenyRemoteInteractiveLogonRight”)
- Deny log on as a batch job (“SeDenyBatchLogonRight”)
- Deny access to this computer from the network (“SeDenyNetworkLogonRight”)

The above settings effectively deny a defined account the ability to be used for interactive or remote logon purposes.

Logging and Hunting

Visibility Goal: Ensure optimized visibility for events associated with Barracuda ESG appliances.

The ESG generates syslog messages (saved as text files) that record activities such as:

- **Web syslog** logs user login activities and any configuration changes made on the appliance.
- **Mail syslog** logs the outcome of each message processed and the reason code associated.

This information is available via the ESG UI `ADVANCED > Troubleshooting` page, although Mandiant recommends using a Syslog server to centrally archive and monitor ESG events.

For additional information related to the Syslog configuration options for an ESG appliance, reference:

https://campus.barracuda.com/product/emailsecuritygateway/doc/3866697/using-a-syslog-server-to-centrally-monitor-system-logs

For hunting, Barracuda has included three (3) YARA rules that can be used to hunt for evidence of the malicious TAR file which exploits CVE-2023-2868:

https://www.barracuda.com/company/legal/esg-vulnerability

Windows Lateral Movement: Architecture Hardening

Identify and Reduce the Scope of Privileged Accounts in Active Directory

MITRE ATT&CK ID: T1078

To reduce the attack surface of an on-premises Active Directory (AD) environment, organizations should proactively **identify** and **attempt to reduce** the scope of accounts that are provided privileged access. Specifically, any Active Directory integrated accounts that can directly interface with Barracuda ESG appliances should not be granted permissions to administer Tier 0 endpoints and applications.

The following built-in Active Directory groups represent a significant level of privileged groups within AD and are often targeted by threat actors for privilege escalation, lateral movement, and persistence.

- `Domain Admins`
- `Enterprise Admins`
- `Schema Admins`
- `Administrators`
- `Account Operators`
- `Backup Operators`
- `Cert Publishers`
- `Print Operators`
- `Server Operators`
- `DNS Admins`
- `Replicator`
- `Group Policy Creator Owners`
- `Denied RODC Password Replication` Group
- `Distributed COM Users`

Using the Active Directory PowerShell cmdlet module, group membership for the aforementioned groups can be enumerated. An example is provided below:

```
get-ADGroupMember -Identity "Domain Admins" -Recursive | export-csv -path <path to csv export>
```

Note: If an organization leverages virtualized infrastructure (on-premises or cloud) to host applications and services, any accounts that provide administrative access to the platforms should also be considered as a "privileged" role. The scope of accounts that are provided this level of access should be reviewed and minimized, in addition to the enforcement of security controls that restrict administrative access to only specific IP addresses / subnets associated with privileged identities.

Reduce the Scope of Permissions Assigned to Privileged Accounts

To inhibit a threat actor's ability to leverage a compromised system or credential to escalate privileges and laterally move within an environment, organizations should review the operational necessity for any accounts that have elevated permissions on endpoints, and work to reduce the scope of privileges assigned to users and services.

Standard user accounts should not require administrative privileges to perform daily job functions and services should operate with the lowest privilege level possible.

Tiered Accounts

All personnel that are assigned administrative responsibilities should utilize separate accounts for administrative functions - that are distinct from normal user accounts.

- **Standard user accounts** - Granted standard user privileges for common user tasks - such as email, web browsing, and using various corporate applications. These accounts should not be granted administrative privileges on endpoints.
- **Administrative (secondary) accounts** - Separate accounts created for personnel who are assigned various tiers of administrative privileges. An administrator who is required to manage assets in each Tier (discussed

below) should utilize a separate account for each Tier. These accounts should not be leveraged to access email or used for web browsing - and should be explicitly restricted to only being leveraged within each Tier.

For secondary accounts that have privileged access (i.e., Enterprise Admin, Domain Admin, Exchange Admin) throughout the environment, these accounts should not be utilized on standard workstations and laptops, but from designated systems (ex: jump boxes) that reside in restricted and protected VLANs and Tiers. Consider blocking any accounts with enterprise and/or domain administrative access from being able to login (remotely or locally) to standard workstations, laptops, and common access servers.

For the group policy object (GPO) settings referenced below, the settings are configurable via the path of:

```
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment
```

Accounts delegated with local or domain privileged access should be explicitly denied access to standard workstations and laptops systems within the context of the following settings (which can be configured using a GPO):

- `Deny access to this computer from the network (SeDenyNetworkLogonRight)`
- `Deny log on as a batch job (SeDenyBatchLogonRight)`
- `Deny log on as a service (SeDenyServiceLogonRight)`
- `Deny log on locally (SeDenyInteractiveLogonRight)`
- `Deny log on through Terminal Services (SeDenyRemoteInteractiveLogonRight)`
- `Debug programs (SeDebugPrivilege) - should be removed for all users - including local administrators`

In addition, organizations should consider designing and staging protected tiered network segments within the environment - and designate these segments as the only authorized origination point from which privileged functions can occur (e.g., remote server administration, database management, application management, Active Directory management, help desk functions). This should be enforced by controls at the network, Active Directory, and endpoint-based layers.

Ideally – the architecture should support various Tiers for access control:

- Tier 0 = Domain Controllers and highly critical services
- Tier 1 = Servers and Hosted Applications
- Tier 2 = User Workstations, Laptops, and common access servers

Additional security controls for consideration:

- Direct access (using administrative and management ports) from Tier 2 systems to Tier 0 systems should be explicitly blocked.
- Specific accounts should only be delegated access to Tier 0 systems (and only initiated from systems within the Tier 0 layer).
- Specific accounts should only be delegated access to Tier 1 systems (and only initiated from systems within the Tier 1 layer).

On Tier 2 systems, accounts delegated for Tier 0 and Tier 1 access should be explicitly denied for access – using the following settings (which can be configured within the context of GPO settings):

- `Deny access to this computer from the network` (also include `S-1-5-114: NT AUTHORITY\Local account and member of Administrators group`)
- `Deny log on as a batch job`

- `Deny log on as a service`
- `Deny log on locally`
- `Deny log on through Terminal Services` (also include `S-1-5-114: NT AUTHORITY\Local account and member of Administrators group)`

On Tier 1 systems, accounts delegated for Tier 0 access should be explicitly denied for access – using the following settings (which can be configured within the context of GPO settings):

- `Deny access to this computer from the network`
- `Deny log on as a batch job`
- `Deny log on as a service`
- `Deny log on locally`
- `Deny log on through Terminal Services`

On Tier 0 systems, only accounts designated for Tier 0 administration purposes should be granted access - using the following settings (which can be configured within the context of GPO settings):

- `Allow log on locally`
- `Allow log on through Terminal Services`

Lateral Movement Tactics and Associated Hardening Controls

Table 1 contains common tactics and the associated hardening controls that can be leveraged to combat against remote access tools and methods from being utilized for lateral movement within an environment.

Tool / Tactic	Mitigating Security Configuration(s)

MITRE ATT&CK ID: T1021.002
PSExec (using the current logged-on user account, without the -u switch)
If the -u switch is not leveraged, authentication will use Kerberos or NTLM for the current logged-on user of the source endpoint – and will register as a Type 3 (network) logon on the destination endpoint.
PSExec – high level functionality:
• Connects to the hidden ADMIN$ share (mapping to the C:\Windows folder) on a remote endpoint via SMB (TCP/445).
• Utilizes the Service Control Manager (SCM) to start the PsExecsvc service and enable a named pipe on a remote endpoint.
• Input/output redirection for the console is achieved via the created named pipe.
	(Mitigating options are listed from least to most impactful)
	Option 1: GPO Configuration
	`Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`
	• `Deny access to this computer from the network`
	Option 2: Windows Firewall Rule enforcement on endpoints
	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`
	Option 3: Disable administrative and hidden shares on endpoints using a GPO.
	`Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)`
	• `Disabled`
	`Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)`
	• `Disabled`

MITRE ATT&CK ID: T1021.002
PSExec (with Alternative Credentials, via the -u switch)
If the -u switch is leveraged, authentication will use the alternate supplied credentials – and will register as a Type 3 (network) and Type 2 (interactive) logon on the destination endpoint.
	Option 1: GPO Configuration
	`Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`
	• `Deny access to this computer from the network`
	• `Deny log on locally`
	Option 2: Windows Firewall Rule enforcement on endpoints
	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`

MITRE ATT&CK ID: T1021.001 Remote Desktop Protocol (RDP)	**Option 1: GPO Configuration** `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`

Tool / Tactic	Mitigating Security Configuration(s)
	- `Deny log on through Terminal Services` **Option 2: Windows Firewall Rule enforcement on endpoints** `netsh advfirewall firewall set rule group="Remote Desktop" new enable=no`

MITRE ATT&CK ID: T1021.006
PS Remoting and WinRM
	Option 1: PowerShell Command
	`Disable-PSRemoting -Force`
	Option 2: GPO Configuration
	`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM`
	- `Disabled`
	Option 3: Windows Firewall Rule enforcement on endpoints
	`netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no`

MITRE ATT&CK ID: T1021.003 Distributed Component Object Model (DCOM)	**Option 1: GPO Configuration** `Computer Configuration > Policies > Windows Settings > Local Policies > Security Options` - `DCOM:Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) Syntax` `Computer Configuration > Policies > Windows Settings > Local Policies > Security Options` - `DCOM:Machine Access Restrictions in Security Descriptor Definition Language (SDDL) Syntax` Both settings allow an organization to define additional computer-wide controls that govern access to all DCOM–based applications on an endpoint. When users or groups that are to be given permission are specified, the security descriptor field is populated with the SDDL representation of those groups and privileges. Users and groups can be given explicit Allow or Deny privileges on both local access and remote access. **Option 2: Windows Firewall Rule enforcement on endpoints (one rule specific to DCOM):**

Tool / Tactic	Mitigating Security Configuration(s)

	`netsh advfirewall firewall set rule name="DFS Management (DCOM-In)" new enable=yes`
	`netsh advfirewall firewall set rule group="DFS Management" new enable=yes`

	(four rules In total should be generated from the above commands)
MITRE ATT&CK IDs: T1563 / T1570 Third-Party Remote Access Applications (e.g., VNC / DameWare / ScreenConnect / AnyConnect)	**Option 1: GPO Configuration** `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment` • `Deny access to this computer from the network` • `Deny log on locally`

Table 1: Common lateral movement tactics and associated hardening controls

MANDIANT
NOW PART OF Google Cloud