Keep mail moving. Control admin access.

One appliance. Preserve evidence references, verify applicable fixes, and name the next owner.

Appliance / inventory reference

Product and model

Response owner

Review date, time, and time zone

1 / MANAGEMENT EXPOSURE AND SERVICE

Management route / port reference

Permitted administrator route / owner

Public admin exposure / evidence reference

Management restriction result

Not checked

Mail delivery and authorized maintenance validation

2 / PRESERVATION AND FIX CONFIRMATION

Preservation decision / collection reference before disruptive changes

Installed firmware / checked time

Applicable patch / support confirmation

Fix confirmation result

Not checked

Use current product-specific vendor instructions. A version string or automatic-update setting alone may not establish patch state. Keep passwords, API keys, raw mail, and full configurations out of this worksheet.

Review the evidence. Own the next step.

Record confirmed observations separately from gaps. New logging only creates future coverage.

Appliance / inventory reference

Review window and time zone

3 / SOURCE COVERAGE

ESG Web syslog: facility, info/debug coverage, retention, and time zone

Firewall / flow / DNS coverage reference

Trusted configuration / change records

Missing coverage / next collection request / owner

Findings and supporting references; approved activity versus unexplained changes

4 / ACTION AND VERIFICATION

Next action and expected result

Action owner and due time

Next review / unresolved question

Verification result / evidence reference

Review outcome: use Unknown until the available evidence supports a result

Not checked

An unexplained change or a management connection is a lead, not proof of this exploit. Escalate suspicious activity through incident response and Barracuda Support. Keep completed copies in your internal incident records.

Open Barracuda's advisory for current patch guidance. Supporting sources: ESG Campus, Mandiant 0041/0042, and CISA KEV.