



# Barracuda Networks ESG Appliance Improper Input Validation Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-2868
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-24 19:15:00 UTC
<b>Updated</b>	2023-06-01 20:14:00 UTC
<b>Description</b>	A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) prod

## Risk And Classification

**EPSS:** 0.907970000 probability, percentile 0.996350000 (date 2026-05-09)

**CISA KEV:** Listed on 2023-05-26; due 2023-06-16; ransomware use Unknown

**Problem Types:** CWE-77

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Barracuda Networks
<b>Product</b>	Email Security Gateway (ESG) Appliance
<b>Name</b>	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://status.barracuda.com/incidents/34kx82j5n4q9">https://status.barracuda.com/incidents/34kx82j5n4q9</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-2868">https://nvd.nist.gov/vuln/detail/CVE-2023-2868</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 300</a>	-	All	All	All
Operating System	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 300 Firmware</a>	All	All	All	All
Hardware	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 400</a>	-	All	All	All
Operating System	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 600</a>	-	All	All	All
Operating System	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 600 Firmware</a>	All	All	All	All
Hardware	<a href="#">Barracuda</a>	<a href="#">Email Security Gateway 800</a>	-	All	All	All

Hardware	Barracuda	Email Security Gateway 800	All	All	All	All
Operating System	Barracuda	Email Security Gateway 800 Firmware	All	All	All	All
Hardware	Barracuda	Email Security Gateway 900	-	All	All	All
Operating System	Barracuda	Email Security Gateway 900 Firmware	All	All	All	All

## References

### Reference

[www.barracuda.com/company/legal/esg-vulnerability](http://www.barracuda.com/company/legal/esg-vulnerability)

Barracuda Networks Status - Barracuda identified a vulnerability (CVE pending) in our Email Security Gateway appliance (ESG) on May 19, 2023

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

150701 Barracuda Email Security Gateway (ESG) Command Injection Vulnerability (CVE-2023-2868)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)