

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **A Zero-Day Vulnerability Found in Barracuda Email Security Gateway**

Date of Publication

May 25, 2023

Admiralty Code

A1

TA Number

TA2023245




# Summary

**First Seen:** May 19, 2023

**Affected Platforms:** Barracuda's Email Security Gateway (ESG)

**Impact:** The exploitation of this zero-day vulnerability could potentially lead to unauthorized access, data breaches, business disruption, financial and reputational damage, and network compromise for affected customers.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-2868	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	Barracuda Networks Email Security Gateway (ESG) Appliance			

# Vulnerability Details

A vulnerability was discovered in the Barracuda Email Security Gateway appliance (ESG) on May 19, 2023, related to the attachment scanning module. This vulnerability existed in a module that initially screens the attachments of incoming emails. Barracuda promptly patched the vulnerability on May 20, 2023, and conducted an investigation. Unauthorized access was found in a subset of email gateway appliances. Subsequently, Barracuda applied a second patch on May 21, 2023, and notified affected users through the ESG user interface. They are actively monitoring the situation, providing updates on their product status page, and reaching out to impacted customers.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-2868	Email Security Gateway (ESG): 5.1.3 - 9.2	cpe:2.3:a:barracuda_networks:esg:9.2:*:*:*:*:*:*	CWE-20

# Recommendations



**Patching and Updates:** Ensure that all Barracuda Email Security Gateway appliances are promptly updated with the necessary security patches to address the vulnerability. Regularly check for updates and apply them as soon as they become available.



**Network Review:** Conduct a thorough review of the network environment to confirm that the threat actors did not spread to other devices or systems. Implement security measures such as network segmentation and access controls to minimize the potential impact of a breach.



**Incident Response and Monitoring:** Establish an incident response plan to effectively respond to any security incidents. Implement robust monitoring mechanisms to detect any suspicious activities or unauthorized access attempts. Continuously monitor the network and appliances for any signs of compromise and take immediate action if any are detected.

## Potential MITRE ATT&CK TTPs

<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0040</u></b> Impact
<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1566</u></b> Phishing
<b><u>T1566.001</u></b> Spearphishing Attachment	<b><u>T1204</u></b> User Execution	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities
<b><u>T1588.005</u></b> Exploits	<b><u>T1203</u></b> Exploitation for Client Execution		

## Patch Details

<https://status.barracuda.com/>  
<https://status.barracuda.com/incidents/34kx82j5n4q9>

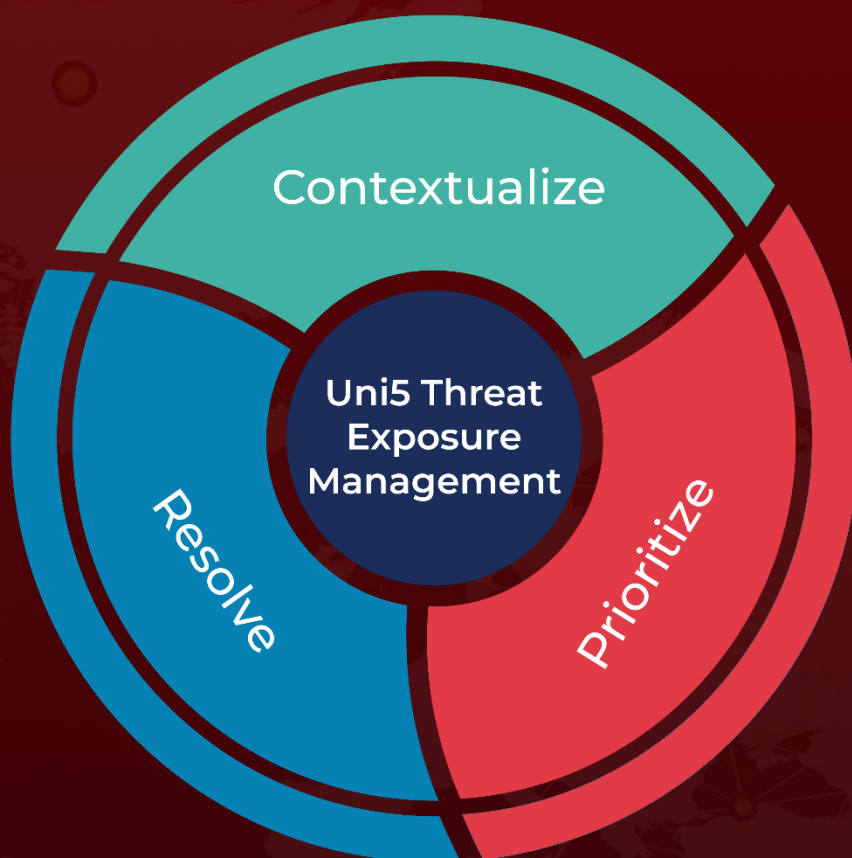
## References

<https://www.barracuda.com/company/legal/esg-vulnerability>  
<https://www.techtarget.com/searchsecurity/news/366538441/Barracuda-discloses-zero-day-flaw-affecting-ESG-appliances>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**May 25, 2023 • 1:30 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)