

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Barracuda Fixes ACE Zero-day Vulnerability Exploited by Attackers

Date of Publication

December 28, 2023

Admiralty Code

A1

TA Number

TA2023524

Summary

First Seen: December 21, 2023







Affected Platform: Barracuda Email Security Gateway (ESG) Appliance and

Malware: SEASPY and SALTWATER

Threat Actor: UNC4841

Impact: The Barracuda Email Security Gateway vulnerability (CVE-2023-7102) allows remote attackers to execute arbitrary commands, posing a substantial threat to the security and functionality of affected systems. Exploitation by threat actors has led to the deployment of new malware variants, emphasizing the severe impact on cybersecurity.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-7102	Barracuda ESG Arbitrary Code Execution Vulnerability	Barracuda Email Security Gateway (ESG) Appliance			
CVE-2023-7101	Spreadsheet::ParseExcel Remote Code Execution Vulnerability	Spreadsheet::Parse Excel			

Vulnerability Details

#1

Barracuda Networks has identified and addressed an Arbitrary Code Execution (ACE) vulnerability, CVE-2023-7102, in their Barracuda Email Security Gateway (ESG) Appliances. This vulnerability allows remote attackers to execute arbitrary commands on the ESG appliance by sending a malicious Excel file. The flaw is associated with the use of the third-party Perl module "Spreadsheet ParseExcel" within the Amavis virus scanner in ESG Appliances.

#2

The vulnerability (CVE-2023-7102) was exploited in the wild by threat actors, and a proof-of-concept exploit is publicly available. Barracuda traced the exploitation to a limited number of ESG devices and linked the activity to the China-based threat actor UNC4841.

#3

Barracuda deployed a security update on December 21, 2023, to automatically address the ACE vulnerability in Spreadsheet::ParseExcel, requiring no customer action. Additionally, on December 22, 2023, Barracuda released a patch to remediate compromised ESG appliances exhibiting indicators of compromise related to new variants of the SEASPY and SALTWATER malware.

#4

CVE-2023-7102 is created by Barracuda for their use of Spreadsheet::ParseExcel, which has been patched. To raise awareness of the ACE vulnerability in Spreadsheet::ParseExcel, Barracuda has also filed CVE-2023-7101.

#5

As of the latest update, there is no known patch or update available for CVE-2023-7101 in the open source library. Organizations using Spreadsheet::ParseExcel in their products or services are advised to review CVE-2023-7101 and promptly take necessary remediation measures. In addition to addressing the CVE-2023-7102 vulnerability, on May 20, 2023, Barracuda Networks also addressed a zero-day vulnerability, CVE-2023-2868, related to Improper Input Validation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-7102	Barracuda's Email Security Gateway (ESG): 5.1.3 - 9.2.1.001	cpe:2.3:a:barracuda:esg_appliance:9.2.1.001:*:*:*:*:*	CWE-1104
CVE-2023-7101	Spreadsheet::ParseExcel version 0.65	cpe:2.3:a:douglas_wilson:spreadsheet_parse_excel:0.65:*:*:*:*:*	CWE-95

Recommendations



Apply Security Updates: Ensure that all Barracuda Email Security Gateway (ESG) Appliances have the latest security update installed. Barracuda Networks has released a patch to address the ACE vulnerability, and it has been automatically applied to active ESGs as of December 21, 2023.



Deploy Anomaly Detection and Monitoring: Implement network monitoring tools with anomaly detection capabilities to identify unusual or suspicious patterns of network activity. This can include unexpected increases in data traffic, unusual access patterns, or deviations from normal behavior.



Network Segmentation: Employ network segmentation to isolate email security appliances from critical internal networks. This can help contain the impact of a potential breach and prevent lateral movement within the network.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities
<u>T1204.002</u> Malicious File	<u>T1203</u> Exploitation for Client Execution	<u>T1588.005</u> Exploits	<u>T1659</u> Content Injection

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2b172fe3329260611a9022e71acdebca, e7842edc7868c8c5cf0480dd98bcfe76, 7b83e4bd880bb9d7904e8f553c2736e3, d493aab1319f10c633f6d223da232a27

TYPE	VALUE
IPv4	23[.]224[.]99[.]242, 23[.]224[.]99[.]243, 23[.]224[.]99[.]244, 23[.]224[.]99[.]245, 23[.]224[.]99[.]246, 23[.]225[.]35[.]234, 23[.]225[.]35[.]235, 23[.]225[.]35[.]236, 23[.]225[.]35[.]237, 23[.]225[.]35[.]238, 107[.]148[.]41[.]146
File Names	ads2[.]xls, don[.]xls, personalbudget[.]xls, wifi-service, mod_tll[.]so
SHA256	803cb5a7de1fe0067a9eeb220dfc24ca56f3f571a986180e146b6cf387855 bdd, 952c5f45d203d8f1a7532e5b59af8e3306b5c1c53a30624b6733e0176d8 d1acd, 118fad9e1f03b8b1abe00529c61dc3edfda043b787c9084180d83535b4d 177b7, 34494ecb02a1cccadda1c7693c45666e1fe3928cc83576f8f07380801b07 d8ba

Patch Details

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

<https://status.barracuda.com/>

References

<https://cert.be/en/advisory/warning-new-exploited-critical-vulnerability-found-barracuda-esg-appliances-successful>

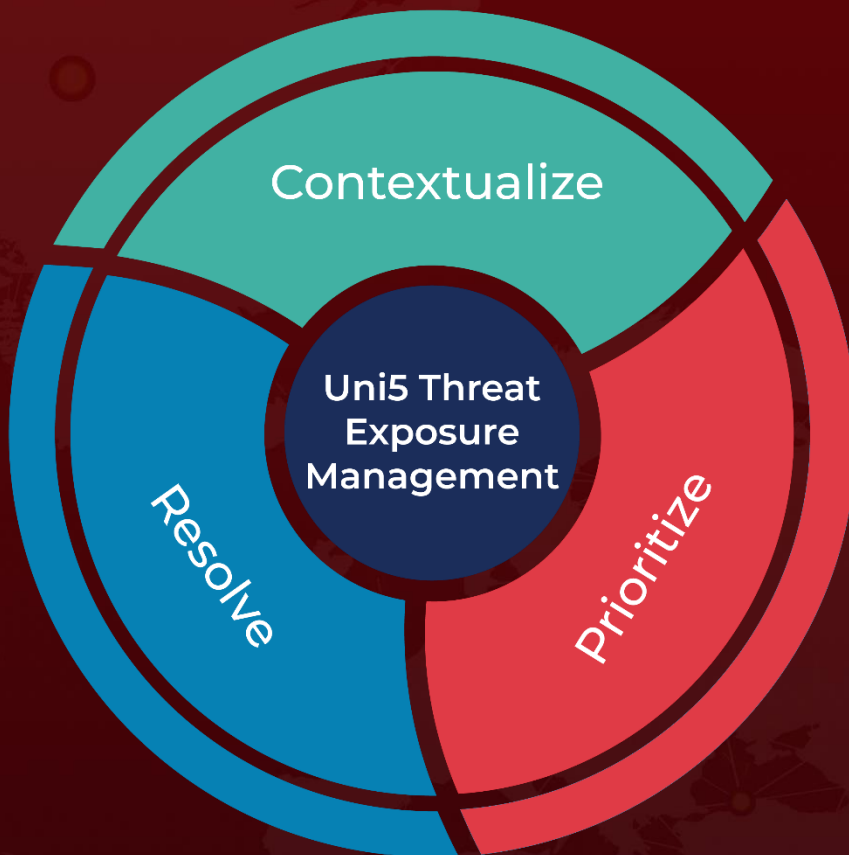
<https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0019.md>

<https://www.hivepro.com/threat-advisory/a-zero-day-vulnerability-found-in-barracuda-email-security-gateway/>

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

December 28, 2023 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro[®]



More at www.hivepro.com