aDvens

Security for the greater good

Newscast
critical vulnerability in Barracuda ESG

2024-01-02 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

BARRACUDA NETWORKS

On December 24, 2023, Barracuda issued an advisory regarding an **exploited** vulnerability in ESG, its email security filtering tool.

Barracuda ESG - CVE-2023-7102

Security researchers discovered a command injection flaw in the third-party library *Spreadsheet::ParseExcel*. The latter is an *open source* library used by the Amavis antivirus within the Barracuda ESG appliance.

Exploitation of this flaw by a remote and unauthenticated attacker allows, by deploying a specifically crafted Excel attachment, to execute arbitrary code.

The publisher mentions that the vulnerability is actively exploited.

Type of vulnerability

- CWE-1104: Use of Unmaintained Third Party Components

Risks

- Arbitrary code execution

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Product impacted

- Barracuda ESG versions up to 5.1.3.001 and 9.2.1.001 (included).

Recommendations

Barracuda deployed out an automatic update to active ESG instances on December 21, 2023. No user action is required.

Based on the observation of the exploitation of the CVE by the APT UNC4841 and the use of new variants of the malwares SEASPY and SALTWATER, the editor deployed a patch on 12/22/2023 on compromised ESG instances presenting IOCs linked to these new variants. No action is required from users.

Barracuda Networks reserved two different CVE IDs:

- The CVE-2023-7101 is dedicated to the vulnerability affecting the Spreadsheet::ParseExcel module alone,
- The CVE-2023-7102 is dedicated to the flaw affecting Barracuda ESG via *Spreadsheet::ParseExcel* and its exploitation.

It is recommended to update the Spreadsheet::ParseExcel module to version 0.66.

Publisher's website

- Additional information is available at Barracuda Bulletin.

Proof of concept

A proof of concept is available as open source.

Sources

BARRACUDA

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

CVE-2023-7102

- https://nvd.nist.gov/vuln/detail/CVE-2023-7102
- https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0019.md
- https://metacpan.org/dist/Spreadsheet-ParseExcel