Date: February 28, 2024

Revision	Date	Changes
1.0	February 28, 2024	Initial release

The CVE-ID tracking this issue: CVE-2024-27889
CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-89: Improper Neutralization of Special Elements used in an SQL Command
This vulnerability is being tracked by NGFW-14509

Description

Multiple SQL Injection vulnerabilities exist in the reporting application of the Arista Edge Threat Management - Arista NG Firewall (NGFW). A user with advanced report application access rights can exploit the SQL injection, allowing them to execute commands on the underlying operating system with elevated privileges.

Arista would like to acknowledge and thank Gereon Huppertz, working with Trend Micro's Zero Day Initiative for responsibly reporting CVE-2024-27889

Vulnerability Assessment

Affected Software

- **Arista Edge Threat Management - Arista NG Firewall Versions**
    - 17.0 and prior

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista Edge Threat Management - Arista NG Firewall (Formerly Untangle)

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS Based Products
    - 7710 Series
    - 720D Series
    - 720XP/722XPM Series

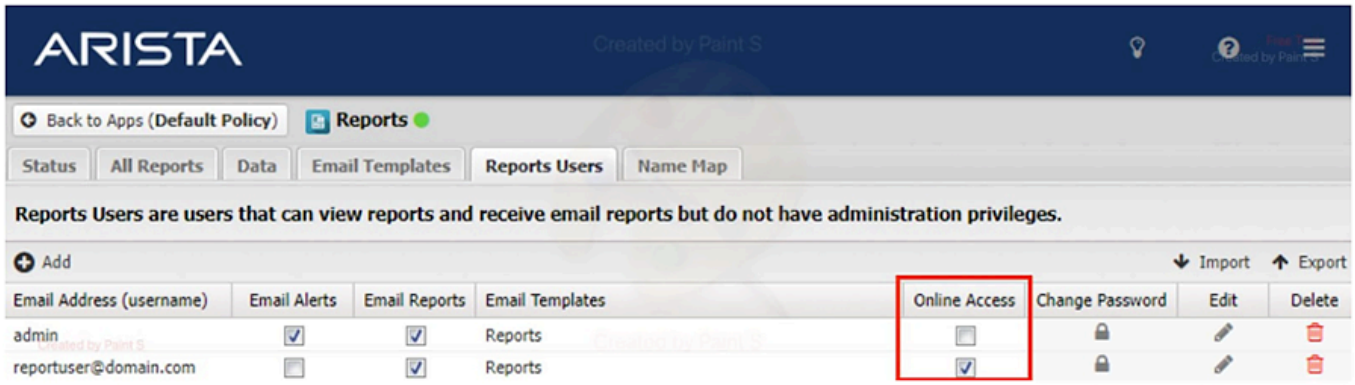
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)

Required Configuration for Exploitation

If the NGFW has one or more Report application Report Users with Online Access enabled they are vulnerable.

To access this information:

1. As the NGFW administrator, log into the UI and navigate to the Reports application.



The above picture shows the configuration panel for user access. The “report” user has “Online Access” checked, which is required in order to be vulnerable.

Indicators of Compromise

Any compromise will reveal itself via the postgres user running a non-standard postgres process.

For example, an appropriate process list for running the postgres database will look like:

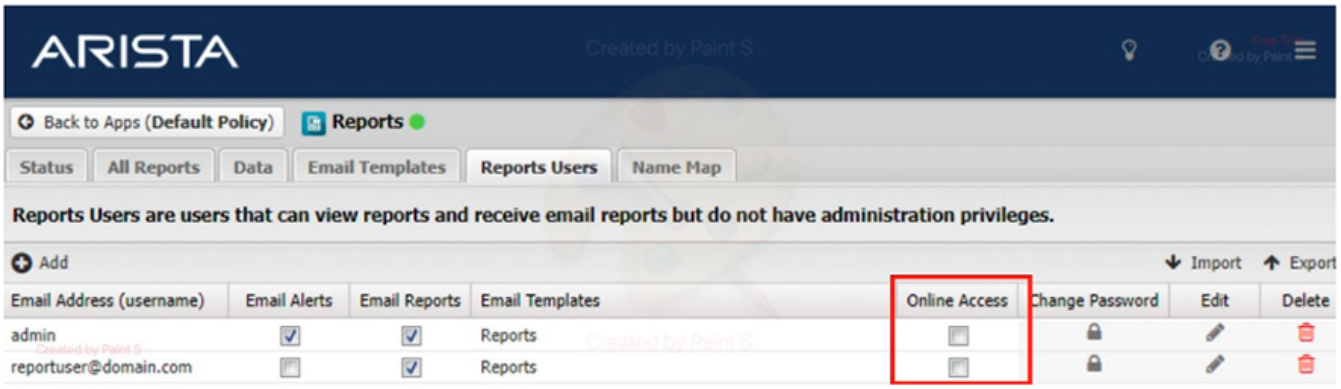
```
# ps -u postgres -f
UID          PID    PPID  C STIME TTY          TIME CMD
postgres   94057       1  0 Feb06 ?        00:00:00 /usr/lib/postgresql/
13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=/etc/pos
tgresql/13/main/postgresql.conf
postgres   94063   94057  0 Feb06 ?        00:00:02 postgres: 13/main: c
heckpointer
postgres   94064   94057  0 Feb06 ?        00:00:00 postgres: 13/main: b
ackground writer
postgres   94065   94057  0 Feb06 ?        00:00:12 postgres: 13/main: w
alwriter
postgres   94066   94057  0 Feb06 ?        00:00:00 postgres: 13/main: a
utovacuum launcher
postgres   94067   94057  0 Feb06 ?        00:00:01 postgres: 13/main: s
tats collector
postgres   94068   94057  0 Feb06 ?        00:00:00 postgres: 13/main: l
ogical replication launcher
```

Additional processes run by the postgres user indicating a potential compromise may look like:

```
postgres 100172 100171  0 Feb06 pts/2    00:00:00 bash
```

Mitigation

For the Reports application, for all Reports Users, disable *Online Access.*



To do this:

2. As the NGFW administrator, log into the UI and go to the Reports application.

3. For all users with the Online Access checkbox (red box) enabled, uncheck it.

4. Click Save.

Resolution

The recommended resolution is to upgrade to the version indicated below and apply the hotfix at your earliest convenience.

- 17.1 Upgrade
- 17.0 (requires Hotfix)

To resolve click the following link for instructions to either upgrading or apply a hotfix patch:
Click here for the hotfix and instructions on resolving this issue

For More Information

If you require further assistance, or if you have any further questions regarding this security

notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

By email: support@arista.com
By telephone: 408-547-5502 ; 866-476-0000
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support