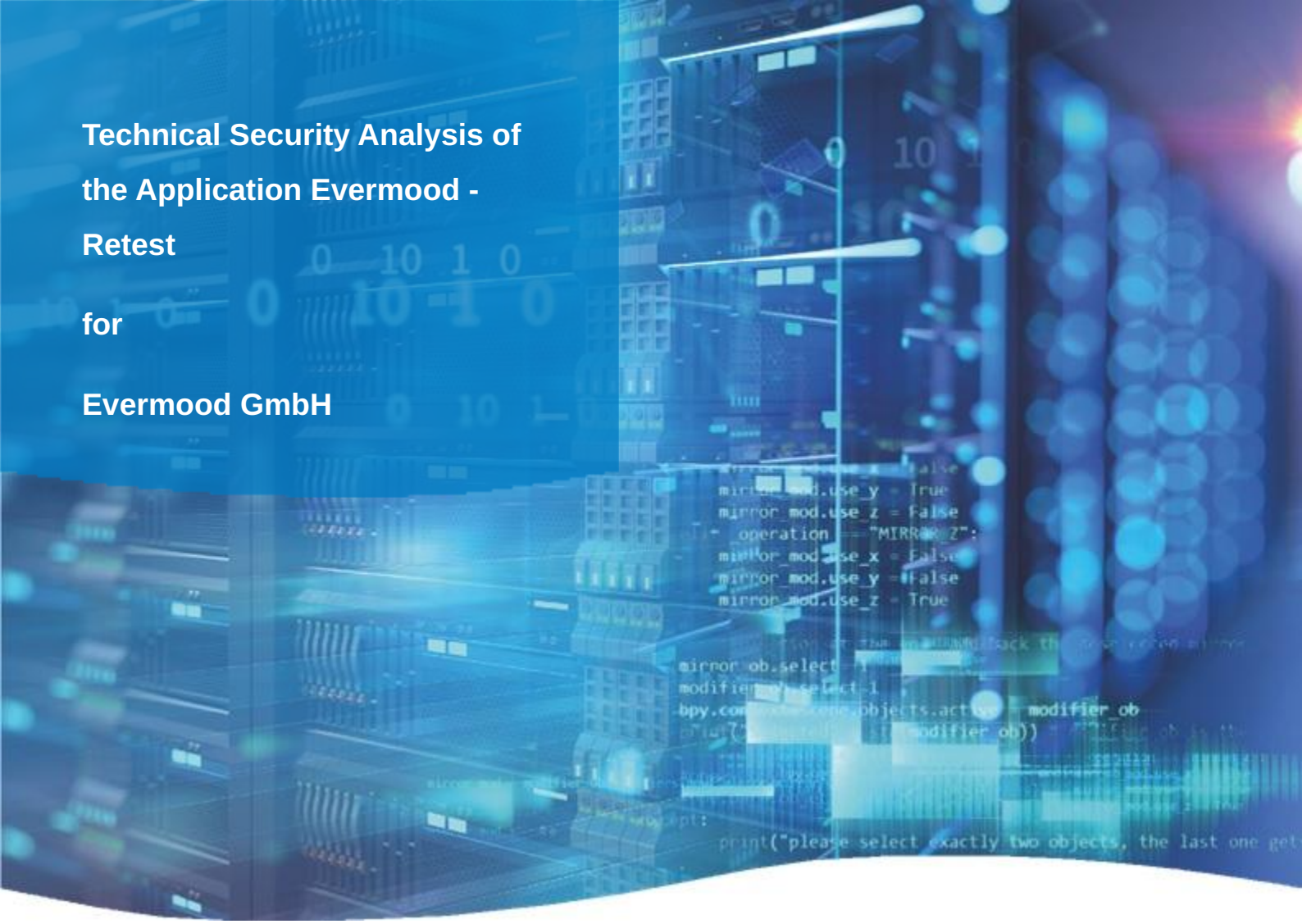

Technical Security Analysis of the Application Evermood - Retest

for

Evermood GmbH

Report

- confidential -

Version 1.1 Final

Report no. 63016945

Cologne, 26.02.2025

TÜV Rheinland i-sec GmbH

www.tuv.com

TÜVRheinland®
Genau. Richtig.

General Information About the Performed Examination

Customer

Evermood GmbH

Rudi-Dutschke-Straße 23 | 10969 Berlin

Contractor

TÜV Rheinland i-sec GmbH

Am Grauen Stein | 51105 Cologne

Freigerichter Straße 1-3 | 63571 Gelnhausen

Dudweilerstraße 17 | 66111 Saarbrücken

Zeppelinstr. 1 | 85399 Hallbergmoos

Köln HRB 30644 | VAT Reg Number: DE812864532

Tel.: +49 221-806 0 | Fax: +49 221-806 2295

E-Mail: service@i-sec.tuv.com

Project Contact

Name	Com-pany	Function	E-mail
Tobias Rohloff	Evermood	Technical and Organizational Contact	Tobias.Rohloff@evermood.com
Raphael Schlegel-berger	TR i-sec	Security Analyst	Raphael.Schlegelberger@i-sec.tuv.com

Project Information

Project name	Technical Security Analysis of the Application Evermood - Retest
Test scope	tuv-pentest.evermood.com
Test environment	Production
Test type / portfolio item	Web application
Test period	19.11.2024 - 26.11.2024
Number of person-days	6 PD
Report template version	5.6.0

Version History

The version history of the document is given below:

Version	Change	Name	Date
0.1	Draft	Raphael Schlegelberger	26.11.2024
1.0	Finalization after suggestions for improvement	Raphael Schlegelberger	09.12.2024
1.1	Adjustments after a retest	Raphael Schlegelberger	20.02.2025

Table of Contents

1 Summary

TÜV Rheinland i-sec GmbH, a member of the TÜV Rheinland Group, has been commissioned by Evermood GmbH (hereinafter referred to as Evermood) with the project *Technical Security Analysis of the Application Evermood - Retest* (*Evermood*).

Objective

A retest was carried out to check whether the weaknesses identified in the previous test had been rectified.

Test Coverage

The original analysis was performed between 19.11.2024 and 26.11.2024. The retest was performed on 20.02.2025.

Result

The following issues could be highlighted positively:

- The application only communicates in encrypted form.
- TÜV Rheinland did not find any issues related to input validation or output coding.
- The retest confirmed that all previously identified vulnerabilities have been fixed.

Overall, the application provides a high level of security in the configuration found.

2 Vulnerability Overview

The following section summarizes the vulnerabilities based on number, severity, and status in graphical as well as tabular form.

2.1 Number of Vulnerabilities by Severity and Status

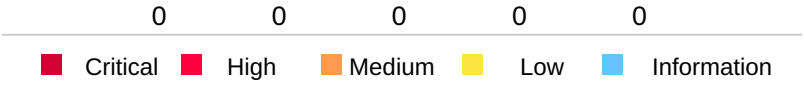

Figure 1 - Open vulnerabilities by severity

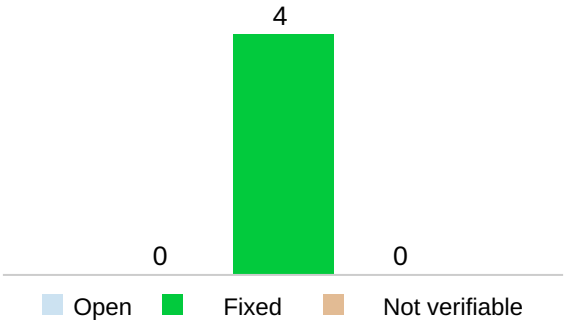

Figure 2 - Vulnerabilities by status

2.2 Tabular Summary of Open Vulnerabilities

Severity	ID	Title

2.3 Tabular Summary of Fixed Vulnerabilities

Severity	ID	Title
LOW	1	Cross-Domain Script Include: tuv-pentest.evermood.com (80.158.47.21) Port 443
	2	Use of Wildcard Certificates: tuv-pentest.evermood.com (80.158.47.21) Port 443
	3	Insecure TLS Configuration: tuv-pentest.evermood.com (80.158.47.21) Port 443
INFORMATION	4	Missing Malware Check for File Uploads: tuv-pentest.evermood.com (80.158.47.21) Port 443

3 Scope and Methodology

This section describes the initial situation, the scope, the objectives, and the basis for testing and evaluating the study.

3.1 Initial Situation and Objectives

TÜV Rheinland i-sec GmbH, a member of the TÜV Rheinland Group, has been commissioned by Evermood GmbH (hereinafter referred to as Evermood) with the project *Technical Security Analysis of the Application Evermood - Retest* (*Evermood*).

A retest was carried out to check whether the weaknesses identified in the previous test had been rectified.

The objective of the analysis was to find vulnerabilities that threaten the confidentiality, integrity, and availability of the systems and applications in scope and the data processed by them.

The analysis was performed between 19.11.2024 and 26.11.2024. A total of 6 person-days were available for the project.

3.2 Test Item

The scope includes the application *Evermood*, a platform for company employees that they can use to access wellness and health services.

The following target systems are in scope of the penetration test:

Description	URL	IP Address
Evermood Website	https://tuv-pentest.evermood.com	80.158.47.21
Evermood Manager Dashboard	https://tuv-pentest.evermood.com/dashboard	80.158.47.21

Out of scope were statistics pages, third-party software like the video player, and the webinar-tool.

The test was conducted in a production environment, which users can access over the Internet.

Evermood provided the following user accounts for the test:

Name	E-Mail	Role
Ansprechperson 1	demo+1@evermood.com	Manager
Ansprechperson 2	demo+2@evermood.com	Manager

3.3 Test Setup

In order to access the systems and applications, TÜV Rheinland used its own testing infrastructure originating from the following prior communicated IP ranges:

IPv4	IPv6
217.243.138.97 – 217.243.138.111	2003:5b:c020::/48
212.18.11.216/29	2001:a60:90dd::/48

To conduct the analysis, the following software components were used:

Software	Version
Burp Suite Professional	2024.9.5
Nmap	7.94SVN
testssl.sh	3.2rc3

Besides the listed tools, TÜV Rheinland used other standard tools that are usually shipped with standard operating systems as well as custom software.

3.4 Test/Audit Fundamentals

The assessment/audit was conducted using the following documents and standards. The assessment focused on the effectiveness of applicable measures rather than the completeness required in these documents and standards:

- OWASP Web Security Testing Guide in version 4.2
- OWASP Top 10 2021
- BSI TR-02102-2 “Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Transport Layer Security (TLS)”
  Additionally, the following resources were used during technical testing to obtain context-related information:
- manufacturer information regarding security weaknesses in the configuration and code (advisories)
- security and context-related information from mailing lists, newsgroups, and forums that is available for the operating systems and application software used
- tools, white papers, and proof-of-concept code to assess the effective security of the operating systems and application software used

3.5 Methodology

3.5.1 Technical Security Analysis of a Web Application

In a preliminary discussion, the scope of the security analysis of the web application(s) is agreed. This includes URLs/IP addresses under which the web application is accessible as well as user credentials in order to be able to analyze the authenticated area of the web application. Subsequently, the web application is examined with dynamic application security testing (DAST) for vulnerabilities which are summarized under the so-called OWASP Top Ten:

- A01:2021 – Broken Access Control
- A02:2021 – Cryptographic Failures
- A03:2021 – Injection

- A04:2021 – Insecure Design
- A05:2021 – Security Misconfiguration
- A06:2021 – Vulnerable and Outdated Components
- A07:2021 – Identification and Authentication Failures
- A08:2021 – Software and Data Integrity Failures
- A09:2021 – Security Logging and Monitoring Failures
- A10:2021 – Server-Side Request Forgery

The procedure for identifying vulnerabilities is based on the OWASP Web Security Testing Guide (WSTG). The WSTG is not limited to tests regarding the OWASP Top Ten, but additionally defines test cases that go beyond the OWASP Top Ten. According to the WSTG, the procedure is divided into a passive and an active phase.
The following paragraphs describes the individual work steps of the passive and active phases.

Passive phase:

Within the passive phase, TÜV Rheinland interacts with the web application to be examined. In doing so, TÜV Rheinland gains an overview of the provided technical functions of the web application as well as the technologies used. The passive phase is supported by the use of tools such as intercepting proxies or tools for enumerating information.
The goal of the passive phase is to determine as much and as detailed information as possible, which helps TÜV Rheinland to better assess the attack surface and subsequently attack as efficiently as possible.

Active phase:

In the second step, the active phase, TÜV Rheinland inspects the web application in scope for vulnerabilities using methods of the WSTG. The aim is to find vulnerabilities that allow an attacker to compromise the confidentiality and integrity of the web application as well as the data it processes.
Depending on the user access levels and permissions provided, TÜV Rheinland also examines the authenticated area of the web application and performs both vertical and horizontal authentication checks. The provision of multiple users with different permissions also increases the depth of the test.
TÜV Rheinland exploits the identified vulnerabilities to obtain further information and possibly deep access to the web application. If successful, TÜV Rheinland uses the newly acquired information to identify any additional vulnerabilities. This phase will pass through iteratively when a vulnerability has been successfully exploited and new information were acquired.
TÜV Rheinland documents identified vulnerabilities within the report.

4 Results in Detail

The following chapter describes the results of the investigation. It also includes recommendations for identified vulnerabilities that sustainably improve or optimize the IT security of the infrastructure, systems, services, and processes in scope.

4.1 Results: Technical Security Analysis of a Web Application

This section summarizes the results of the web application analysis. Manual as well as automated tests were performed for the analysis. Primary tool used for the analysis was *Burp Suite Professional*.

4.1.1 Cross-Domain Script Include

Summary

Problem	So-called cross-domain script includes lead to the situation where the application's security is also dependent on the dynamically included code.
Impact	An attacker that is, e.g., able to manipulate the dynamically included code can attack clients, e.g., by stealing session information to impersonate a legitimate user.
Fix	Script files should not be included from external sources. If that cannot be avoided, Subresource Integrity (SRI) should be used.

Description and Impact

When script files, e.g., JavaScript files are included from an external source, the content of the included file is not under the control of the application's operator. Therefore, the application's security is not only controlled by the application's operator but instead is also dependent on the dynamically included code.

Despite this risk, it is quite common to include script files from external sources. Especially, contractors which offer, e.g., tracking functionality demand from their customers the inclusion of their script code. Hereby, a client dynamically requests the corresponding script code from various external sources, e.g., from the tracking provider itself.

As a result of so-called cross-domain script includes, the risk arises that the included script file contains malicious code that, in the end, will run in the user's application context. There is not only the risk that the service provider of the script code himself puts malicious code into the script file but rather that the provider himself becomes the victim of an attack in which the hosted file gets compromised. In a successful attack, the malicious code can then, among other things, trigger arbitrary functions in the application context or steal session cookies for an impersonation theft.

General Recommendation

Script files should not be included dynamically but instead be hosted locally. This way, the script code is under the control of the application's operator. If the script code is loaded dynamically from external sources, the corresponding resources should only be loaded via a secure channel, e.g., HTTPS. Furthermore, the provided script code should constantly be reviewed according to changes.

If that cannot be avoided, Subresource Integrity (SRI) should be used, which enables browsers to verify that resources they fetch are delivered without unexpected manipulation. This works by adding a tag in form of a cryptographic hash to the script, as shown in the following example:

```
<script src="https://example.com/example-framework.js"
 integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"></
script>
```

References

Further information can be found at the following URLs:

- https://portswigger.net/KnowledgeBase/issues/Details/00500500_Crossdomainscriptinclude
- https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
- https://cwe.mitre.org/data/definitions/829.html

4.1.1.1 [1] - Evidence - tuv-pentest.evermood.com (80.158.47.21) Port 443

Severity	Low
State	**FIXED**
ID	1
Component	tuv-pentest.evermood.com (80.158.47.21:443)
CVSSv3.1	3.7 [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N]

The application includes JavaScript code from the following external source:

- https://player.3qsdn.com/js3q.latest.js

The inclusion takes place at least at the following locations:

- /
- /chat
- /confidants
- /dashboard
- /dashboard/concerns
- /dashboard/login
- /dashboard/marketplace
- /dashboard/statistics/platform

Retest on 20.02.2025

In the retest, it was determined that the JavaScript code, which was previously included from another domain, is now hosted locally.

This is shown in the following client-server-communication.

Request:

```
GET /confidants/095f21fa2e8943059485d08c779e7aea HTTP/2
Host: tuv-pentest.evermood.com
[..SNIP..]
```

Response:

```
HTTP/2 200 OK
Date: Thu, 20 Feb 2025 14:23:11 GMT
Content-Type: text/html; charset=utf-8
[..SNIP..]

<!DOCTYPE html>
<html lang="en-DE" class="scroll-padding-block">
  <head>
    <link rel="stylesheet" href="/vite/assets/tailwind-CHQ5Y-J_.css" media="all" data-
turbo-track="reload" />

[..SNIP..]

<script src="/vite/assets/application-DI4v4wI5.js" crossorigin="anonymous"
type="module" data-turbo-track="reload"></script><link rel="modulepreload" href="/vite/
assets/activestorage.esm-Dd1PED-U.js" as="script" crossorigin="anonymous" data-turbo-
track="reload">

      <script src="/vite/assets/service_worker_register-BZMmjHhT.js" crossori-
gin="anonymous" type="module"></script><link rel="modulepreload" href="/vite/assets/
supports-es6-B18lW2T4.js" as="script" crossorigin="anonymous">


<script src="/js3q.5.3.31.js"></script>

  </head>

  <body data-locale="en">

[..SNIP..]
```

4.1.2 Use of Wildcard Certificates

Summary

Problem	The tested application uses a wildcard certificate.
Impact	An attacker who can obtain this certificate can decrypt the transmitted data for any sub-domain and probably access sensitive information.
Fix	If no central load balancer terminates the TLS traffic for any affected subdomain, a dedicated TLS certificate should be issued for every subdomain.

Description and Impact

While establishing a secured connection with SSL/TLS, the server is required to provide a certificate to prove that he is the targeted system. The client will check the provided certificate to ensure that it was signed by a trusted certificate authority (CA), is valid on the current date, and has not been revoked yet. Thus, the client already is equipped with several pre-installed CAs.
Because the deployed certificate contains a wildcard, an attacker with access to the certificate can read the transmitted clear text data for arbitrary subdomains via a man-in-the-middle attack.

General Recommendation

If no central load balancer terminates the TLS traffic for the affected subdomains, a dedicated TLS certificate should be issued for every subdomain.

References

Further information can be found at the following URLs:

- https://venafi.com/blog/wildcard-certificates-make-encryption-easier-but-less-secure/
- https://www.keyfactor.com/blog/wildcard-certificate-risks/

4.1.2.1 [2] - Evidence - tuv-pentest.evermood.com (80.158.47.21) Port 443

Severity	Low
State	**FIXED**
ID	2
Component	tuv-pentest.evermood.com (80.158.47.21:443)
CVSSv3.1	3.7 [CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N]

The following listing shows an excerpt of the scan results of *testssl.sh* for the domain *tuv-pen-test.evermood.com* on port *443*. The weaknesses in the configuration are marked yellow.

```
[...]
 Testing server defaults (Server Hello)
[...]
 Common Name (CN)             *.evermood.com  (request w/o SNI didn't succeed)
 subjectAltName (SAN)         *.evermood.com
[...]
```

Retest on 20.02.2025

The developer of the application has provided the following information on the use of the wildcard certificate:

> "*A central load balancer is in place to terminate TLS traffic for all subdomains, ensuring that certificate management is centralized and secure. The subdomains are used within the main application to support multi-tenancy, and all services operating under the domain reside within the same cluster. Since traffic is consistently routed through the same reverse proxy, issuing individual certificates for subdomains would not provide any additional security benefit. Therefore, the use of a wildcard certificate in this architecture does not introduce a meaningful security risk.*"

Based on this information, the vulnerability is considered fixed.

4.1.3 Insecure TLS Configuration

Summary

Problem	There are deficits in the configuration of TLS-based encryption.
Impact	This might be useful for an attacker who was able to gain a man-in-the-middle position and hence can decrypt or manipulate the transmitted data to gain sensitive information.
Fix	TÜV Rheinland recommends revising the TLS configurations according to the recommendations of the German Federal Office for Information Security (BSI).

Description and Impact

The configuration of the TLS-based encryption contains deficits that might enable an attacker located between server and client to eavesdrop and decrypt or even alter the transmitted communication. This type of attack in a so-called man-in-the-middle position could become feasible due to weaknesses in the configuration of the deployed TLS components. The identified configuration appears to be deficient compared with acknowledged recommendations, i.e., by the *German Federal Office for Information Security* (BSI).

Below, the identified flaws will be described in detail.

Support of Algorithms not Recommended by BSI
The server supports encryption algorithms that are not recommended by the BSI. The BSI does not explicitly dissuade support of these ciphers but does not recommend their use either.

Support of Gzip Compression
If data is compressed on application layer before being encrypted in order to reduce the transmitted amount of data, parts of the plain text are easier to guess for an attacker. Hence, he might be able to recover even more plain text by mounting a known-plaintext attack on the cipher text. This attack has been demonstrated in the past, especially by the BREACH attack.

General Recommendation

The BSI regularly publishes recommendations with regard to the use of state-of-the-art cryptography. In their technical guideline TR-02102-02 (version 2024-01) from January 2024, the BSI recommends the following cipher suites for use with TLSv1.2.

	Key Exchange and Authentication		Symmetric Encryption Algorithm	Mode of Operation	Hash Algorithm	Use Until
TLS	ECDHE ECDSA	WITH	AES 128	CBC	SHA256	2030+
TLS	ECDHE ECDSA	WITH	AES 256	CBC	SHA384	2030+
TLS	ECDHE ECDSA	WITH	AES 128	GCM	SHA256	2030+
TLS	ECDHE ECDSA	WITH	AES 256	GCM	SHA384	2030+
TLS	ECDHE ECDSA	WITH	AES 128	CCM		2030+
TLS	ECDHE ECDSA	WITH	AES 256	CCM		2030+
TLS	ECDHE RSA	WITH	AES 128	CBC	SHA256	2030+
TLS	ECDHE RSA	WITH	AES 256	CBC	SHA384	2030+
TLS	ECDHE RSA	WITH	AES 128	GCM	SHA256	2030+
TLS	ECDHE RSA	WITH	AES 256	GCM	SHA384	2030+
TLS	DHE DSS	WITH	AES 128	CBC	SHA256	2029
TLS	DHE DSS	WITH	AES 256	CBC	SHA256	2029
TLS	DHE DSS	WITH	AES 128	GCM	SHA256	2029
TLS	DHE DSS	WITH	AES 256	GCM	SHA384	2029
TLS	DHE RSA	WITH	AES 128	CBC	SHA256	2029
TLS	DHE RSA	WITH	AES 256	CBC	SHA256	2029
TLS	DHE RSA	WITH	AES 128	GCM	SHA256	2029
TLS	DHE RSA	WITH	AES 256	GCM	SHA384	2029
TLS	DHE RSA	WITH	AES 128	CCM		2029
TLS	DHE RSA	WITH	AES 256	CCM		2029

The BSI recommends the following cipher suites with TLSv1.3.

	Key Exchange and Authentication		Symmetric Encryption Algorithm	Mode of Operation	Hash Algorithm	Use Until
TLS	DHE/ECDHE	WITH	AES 128	GCM	SHA256	2030+
TLS	DHE/ECDHE	WITH	AES 256	GCM	SHA384	2030+
TLS	DHE/ECDHE	WITH	AES 128	CCM	SHA256	2030+

References

Further information can be found at the following URLs:

- https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf
- https://blog.qualys.com/ssllabs/2011/10/31/tls-renegotiation-and-denial-of-service-attacks
- https://cwe.mitre.org/data/definitions/326.html

4.1.3.1 [3] - Evidence - tuv-pentest.evermood.com (80.158.47.21) Port 443

Severity	Low
State	**FIXED**
ID	3
Component	tuv-pentest.evermood.com (80.158.47.21:443)
CVSSv3.1	3.7 [CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N]

The following listing shows an excerpt of the scan results of *testssl.sh* for the domain *80.158.47.21* on port *443.* Weak cipher suites and algorithms are marked yellow while hints are highlighted in blue.

```
[...]
 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits
------------------------------------------------------------------------------
SSLv2
[...]
SSLv3
[...]
TLSv1
[...]
TLSv1.1
[...]
TLSv1.2 (server order)
[...]
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20   256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
[...]
TLSv1.3 (server order)
[...]
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20   256
TLS_CHACHA20_POLY1305_SHA256
[...]
 Testing vulnerabilities
[...]
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression
detected. - only supplied "/" tested
[...]
```

Retest on 20.02.2025

In the retest, it was determined that only algorithms recommended by the BSI are used. This is shown in the following excerpt from the *testssl* tool:

```
[...]

TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

```
 x9e     DHE-RSA-AES128-GCM-SHA256          DH 4096    AESGCM      128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 x9f     DHE-RSA-AES256-GCM-SHA384          DH 4096    AESGCM      256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.3 (server order)
 x1302   TLS_AES_256_GCM_SHA384             ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1301   TLS_AES_128_GCM_SHA256             ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256

[...]
```

4.1.4 Missing Malware Check for File Uploads

Summary

Problem	The restrictions implemented by the application for uploaded files are incomplete.
Impact	Attackers can therefore upload files that may contain malicious code. This may result in the user who downloads such a file executing the malicious code.
Fix	The application should check files for malicious code before uploading.

Description and Impact

During the tests, the absence of antivirus software was demonstrated with the EICAR test file. The EICAR test file is not a virus but a file developed by the *European Institute for Computer Anti-Virus Research e.V.* association. This file contains an ASCII string test pattern which is recognized as such by common virus scanners. If the test pattern is detected, the virus scanner executes the usual antivirus software instructions and processes for handling a virus file.

General Recommendation

The application should scan files for malicious code when uploading. If potential malware is detected, the file should not be accepted for upload by the application and the user should be warned with an appropriate error message. Alternatively, the check could also be performed when downloading the affected file. In both cases, the malicious code must not be delivered to the user.

References

Further information can be found at the following URLs:

- https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
- https://www.eicar.org/download-anti-malware-testfile/

4.1.4.1 [4] - Evidence - tuv-pentest.evermood.com (80.158.47.21) Port 443

Severity	Information
State	**FIXED**
ID	4
Component	tuv-pentest.evermood.com (80.158.47.21:443)
CVSSv3.1	0.0 [CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:N]

Managers of the application can create events for employees. They are able to upload files to provide additional information, which can then be downloaded by users. TÜV Rheinland has determined that there is no malware check for these files. The following client-server communication shows the upload of the of the EICAR file.

Request:

```
POST /dashboard/events/custom_events/999c4183b1364de4a959ac8fd1595796 HTTP/2
Host: tuv-pentest.evermood.com
[...]
Content-Type: multipart/form-data; bound-
ary=---------------------------387416959321107183197350947 36
Content-Length: 3006
Origin: https://tuv-pentest.evermood.com
Dnt: 1
Sec-Gpc: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

[...]

true
-----------------------------387416959321107183197350947 36
Content-Disposition: form-data; name="custom_event[attachment]"; filename="eicar.com"
Content-Type: application/x-msdos-program

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
-----------------------------387416959321107183197350947 36
Content-Disposition: form-data; name="custom_event[attachment_type]"

document
-----------------------------387416959321107183197350947 36
Content-Disposition: form-data; name="commit"

Save
-----------------------------387416959321107183197350947 36--
```

Response:

```
HTTP/2 200 OK
Date: Mon, 25 Nov 2024 15:41:35 GMT
[...]

<turbo-stream action="prepend" target="flashes"><template>
[...]
    <p class="ml-2 text-sm font-medium text-green-800">All changes have been saved.</p>
[...]
<div class="flex flex-col space-y-1">
    <span class="block text-sm font-medium text-gray-700">Uploaded files</span>

      <div class="flex flex-row w-full p-2 gap-1 items-center justify-between bg-
gray-100 rounded-md" data-test="uploaded-file">
        <span class="grow overflow-hidden truncate text-sm">eicar.com</span>
        <div class="flex flex-row max-w-fit gap-2">

    <a class="group relative p-1.5 bg-transparent text-gray-800 hover:bg-gray-100
hover:text-gray-900 active:bg-gray-200 aria-disabled:border-transparent aria-dis-
abled:bg-gray-100 aria-disabled:text-gray-400 gap-x-1.5 inline-flex items-center
```

```
rounded text-sm font-medium cursor-pointer aria-disabled:cursor-not-allowed text-center
justify-center" role="button" aria-label="Download file" href="/rails/active_storage/
blobs/redirect/eyJfcmFpbHMiOnsiZGF0YSI6MTI4ODIxLCJwdXIiOiJibG9iX2lkIn19--fe065707ce66b-
dc56dd5f64c45c91c27949bfd2d/eicar.com?disposition=attachment">
```

When visiting the corresponding event page (no user needed), it is possible to download the EICAR file. After a redirect, the user downloads the file from an external domain, as the following request shows:

```
GET /zqcv3zp5bhxh4ohewnum798ge14j?response-content-disposi-
tion=attachment%3B%20filename%3D%22eicar.com%22%3B%20filename%2A%3DUTF-8%27%27eicar.com
&response-content-type=application%2Fx-msdos-program&X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Credential=WXOXRHHWFXHJKZIX7I0U%2F20241125%2Feu-de%2Fs3%2Faws4_request&X-
Amz-Date=20241125T154232Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signa-
ture=36e3d7d6bbdb03d7f31e85b91c7f4f0373c96cc76da1a6eeaa78dc86807fdf70 HTTP/1.1
Host: evermood-server-app-data-production.obs.eu-de.otc.t-systems.com
```

Response:

```
HTTP/1.1 200 OK
Server: OBS
x-reserved: amazon, aws and amazon web services are trademarks or registered trademarks
of Amazon Technologies, Inc
x-amz-request-id: 0000019363FD1DFB60897406BC36E866
Content-MD5: RNiGEv6oqPNt6C4SeKuwLw==
Accept-Ranges: bytes
ETag: "44d88612fea8a8f36de82e1278abb02f"
Last-Modified: Mon, 25 Nov 2024 15:41:35 GMT
Content-Disposition: attachment; filename="eicar.com"; filename*=UTF-8''eicar.com
x-amz-version-id: G001119363FC3ED7000049D5099CC065
Content-Type: application/x-msdos-program
x-amz-tagging-count: 0
x-amz-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Date: Mon, 25 Nov 2024 15:42:32 GMT
Content-Length: 68

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Retest on 20.02.2025

The application now checks files for malicious code directly during upload and issues an error message if this is the case. This is shown in Figure 3 .

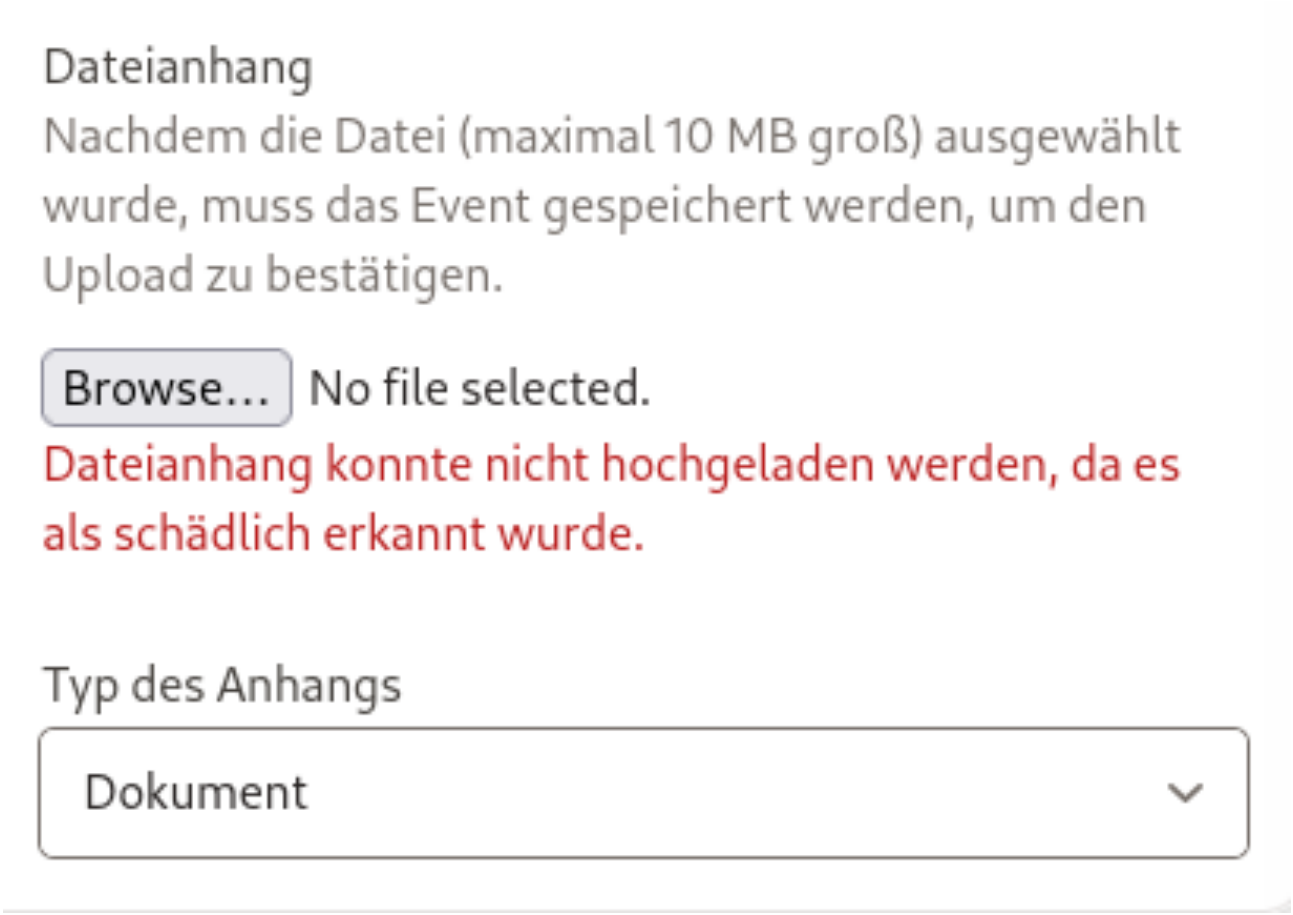

Figure 3 - Failed file upload due to malicious code detection

5 General Remarks

In a security audit, the results base on self-disclosed information in the form of discussions with the responsible employees and spot checks of configurations on the relevant systems. Both are limited in terms of scope and time horizon.

In a technical security analysis, the testers identify security-relevant information directly. In principle, testers can only identify security vulnerabilities but not prove their absence.

Despite the greatest possible care, in both cases, not all security aspects might be unveiled. TÜV Rheinland i-sec GmbH therefore excludes any liability for existing but unidentified risks.

The results of the investigation do not in any way release Evermood from pursuing their security objectives. In any case, Evermood is responsible for implementing measures to eliminate vulnerabilities and pursue their security objectives.

Any liability for possible damages resulting from incorrect implementation of the provided information is excluded.

A Attachment

A.1 Assessment Basics and Vulnerability Classification

TÜV Rheinland divides the findings of the analysis into five categories, which are defined in the following tables. Our experts classify the identified vulnerabilities from an IT security perspective related to the infrastructure, systems, services, and processes under investigation. An equivalent risk to the company's business processes cannot be derived directly from these valuations. The client's risk management department must assess the resulting risk for their company themselves.

In addition, each finding is evaluated according to the standard Common Vulnerability Scoring System version 3.1 (CVSSv3.1). This scoring scheme usually evaluates the severity of a vulnerability under different aspects, which can lead to discrepancies in the severity rating between the two systems.

A.1.1 Classification Level "Critical"

Criteria	Rating	Description
Impact	Critical	An attacker is able to compromise the entire infrastructure or IT system and massively disrupt the protection goals.
Attack complexity	Low	A successful attack requires a low level of effort or presupposes a low level of technical knowledge for the attacker.
Probability	High to very high	There is a high or very high probability that the vulnerability will be exploited by an attacker.
User interaction	Not required	User interaction is usually not required.
Need for action	Urgently required	The vulnerability must be fixed immediately as there exists a significant security risk to the infrastructure or user data on the system.

A.1.2 Classification Level "High"

Criteria	Rating	Description
Impact	Serious	An attacker can compromise key parts of the infrastructure or IT system and disrupt the protection objectives.
Attack complexity	Low to medium	A successful attack requires a low level of effort or assumes a low level of technical knowledge for the attacker.
Probability	High	There is an increased probability that the vulnerability will be exploited by an attacker.
User interaction	Mostly not required	User interaction is often not required.
Need for action	Urgently required	The vulnerability needs to be fixed promptly as there is a high security risk to the infrastructure or users of the system.

A.1.3 Classification Level "Medium"

Criteria	Rating	Description
Impact	Medium	An attacker is able to compromise parts of the infrastructure or IT system and disrupt the protection goals.
Attack complexity	Medium	A successful attack requires low/high effort or requires high/low technical knowledge for the attacker.
Probability	Medium	There is a probability that the vulnerability will be exploited by an attacker.
User interaction	Mostly Required	User interaction is often required.
Need for action	Required in a timely manner	The vulnerability should be fixed because there is a medium security risk to the infrastructure or users of the system.

A.1.4 Classification Level "Low"

Criteria	Rating	Description
Impact	Low	An attacker can possibly compromise parts of the infrastructure or IT system and possibly disrupt the protection goals.
Attack complexity	High	A successful attack requires a high level of effort and technical knowledge for the attacker.
Probability	Low	There is a low probability that the vulnerability will be exploited by an attacker.
User interaction	Mostly required	User interaction is usually required.
Need for action	Required in the future	The vulnerability should be fixed in the future as there is a low security risk to the infrastructure or the users of the system.

A.1.5 Classification Level "Information"

Criteria	Rating	Description
Impact	None	An attacker can obtain information from the target system or potentially trigger unwanted behavior.
Attack complexity	Situational	It depends on the situation whether it is difficult or easy to trigger the behavior or to obtain the information. Most of the time, however, this is easy to accomplish.
Probability	Situational	The probability that the behavior will be exploited usually depends on its complexity.
User interaction	Mostly not required	User interaction is often not required.
Need for action	Mostly not required	Check in the future if the behavior or information disclosure is desired or can be turned off.

A.2 Detailed results of the port scan

A.2.1 80.158.47.21

IP-Address

80.158.47.21

Hostname

tuv-pentest.evermood.com

Overview of the Ports

Protocol	Port	Name	State	Product	Reason	Version
tcp	80	http	open	nginx	syn-ack	
tcp	443	https	open	nginx	syn-ack	
tcp	3544	teredo	closed		reset	

A.3 Detailed TLS Scan Results

The following is scan data for each system.

A.3.1 tuv-pentest.evermood.com (80.158.47.21) Port 443

```
## Scan started as: "testssl --log tuv-pentest.evermood.com"
## at kali:/usr/bin/openssl
## version testssl: 3.2rc3  from
## version openssl: "3.3.2" from "Oct 27 14:19:50 2024")

 Start 2024-11-19 15:03:33               -->> 80.158.47.21:443 (tuv-pen-
test.evermood.com) <<--

 rDNS (80.158.47.21):    ecs-80-158-47-21.reverse.open-telekom-cloud.com.
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            not offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits
------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
```

```
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 x9e     DHE-RSA-AES128-GCM-SHA256         DH 4096    AESGCM      128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 x9f     DHE-RSA-AES256-GCM-SHA384         DH 4096    AESGCM      256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.3 (server order)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20    256
TLS_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256

 Has server cipher order?     yes (OK) -- TLS 1.3 and below


 Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES,
RC4

 FS is offered (OK)           TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384
                              ECDHE-RSA-CHACHA20-POLY1305 TLS_AES_128_GCM_SHA256 ECDHE-
RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256
 Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519 X448
 Finite field group:          ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192
 TLS 1.2 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-
RSAE+SHA512 RSA+SHA256 RSA+SHA384 RSA+SHA512 RSA+SHA224
 TLS 1.3 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-PSS-
RSAE+SHA512

 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281" "server name/#0" "EC point
formats/#11" "supported versions/#43" "key share/#51"
                              "max fragment length/#1" "application layer protocol
negotiation/#16" "extended master secret/#23"
 Session Ticket RFC 5077 hint no -- no lifetime advertised
 SSL Session ID support       yes
 Session Resumption           Tickets no, ID: no
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      none
 Client Authentication        none
 Signature Algorithm          SHA256 with RSA
 Server key size              RSA 2048 bits (exponent is 65537)
 Server key usage             Digital Signature, Key Encipherment
 Server extended key usage    TLS Web Server Authentication, TLS Web Client Authentica-
tion
 Serial                       03EBACE20A0C9E2C8B75DA099266D855C499 (OK: length 18)
 Fingerprints                 SHA1 70676C19863BDC0C04EDF65D32937F19D296880D
                              SHA256
8D507C9F2526D6489662A19611F599E9358D3A5FEB76088A38C306D7052C492E
 Common Name (CN)             *.evermood.com  (request w/o SNI didn't succeed)
 subjectAltName (SAN)         *.evermood.com
 Trust (hostname)             Ok via SAN wildcard and CN wildcard (SNI mandatory)
```

```
 Chain of trust                Ok
 EV cert (experimental)        no
 Certificate Validity (UTC)    67 >= 30 days (2024-10-28 09:54 --> 2025-01-26 09:54)
 ETS/"eTLS", visibility info   not present
 Certificate Revocation List   --
 OCSP URI                      http://r11.o.lencr.org
 OCSP stapling                 not offered
 OCSP must staple extension    --
 DNS CAA RR (experimental)     available - please check for match with "Issuer" below
                               issue=letsencrypt.org, issuewild=;
 Certificate Transparency      yes (certificate extension)
 Certificates provided         2
 Issuer                        R11 (Let's Encrypt from US)
 Intermediate cert validity    #1: ok > 40 days (2027-03-12 23:59). R11 <-- ISRG Root X1
 Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code              200 OK
 HTTP clock skew               0 sec from localtime
 Strict Transport Security     365 days=31536000 s, includeSubDomains
 Public Key Pinning            --
 Server banner                 (no "Server" line in header, interesting!)
 Application banner            --
 Cookie(s)                     2 issued: 2/2 secure, 2/2 HttpOnly
 Security headers              X-Frame-Options: SAMEORIGIN
                               X-Content-Type-Options: nosniff
                               Content-Security-Policy: default-src 'self' https:;
script-src 'self' https: blob: https://*.3qsdn.com
                                'nonce-eIwfm0fjd0ahZub4HhrV5Q==';  style-src 'self'
https: 'unsafe-inline'; font-src 'self' https: data:;
                                object-src 'none'; connect-src 'self' https: wss: data:
https://*.3qsdn.com
                                https://evermood-server-app-data-production.obs.eu-
de.otc.t-systems.com; media-src 'self' https: blob:
                                https://*.3qsdn.com https://evermood-server-app-data-
production.obs.eu-de.otc.t-systems.com; img-src 'self' https:
                                data: https://evermood-server-app-data-produc-
tion.obs.eu-de.otc.t-systems.com; frame-ancestors 'self'
                               Permissions-Policy: geolocation=(), camera=(), micro-
phone=(), payment=(), display-capture=()
                               X-XSS-Protection: 0
                               Referrer-Policy: strict-origin-when-cross-origin
                               Cache-Control: no-store
                               Pragma: no-cache
 Reverse Proxy banner          --


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket
extension
 ROBOT                                     Server does not support any cipher suites
that use RSA key transport
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression
detected. - only supplied "/" tested
                                           Can be ignored for static pages or if no
secrets in the page
```

```
 POODLE, SSL (CVE-2014-3566)              not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)             No fallback possible (OK), no protocol below
TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)   not vulnerable (OK)
 FREAK (CVE-2015-0204)                    not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)     not vulnerable on this host and port (OK)
                                          make sure you don't use this certificate
elsewhere with SSLv2 enabled services, see
                                          https://search.censys.io/search?
resource=hosts&virtual_hosts=INCLUDE&q=8D507C9F2526D6489662A19611F599E9358D3A5FEB76088A
38C306D7052C492E
 LOGJAM (CVE-2015-4000), experimental     not vulnerable (OK): no DH EXPORT ciphers,
no common prime detected
 BEAST (CVE-2011-3389)                    not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental    not vulnerable (OK)
 Winshock (CVE-2014-6321), experimental   not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)       no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward
Secrecy
------------------------------------------------------------------------------------
---------
 Android 6.0                  TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Android 7.0 (native)         TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Android 8.1 (native)         TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 Android 9.0 (native)         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 10.0 (native)        TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 11 (native)          TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 12 (native)          TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Chrome 79 (Win 10)           TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Chrome 101 (Win 10)          TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Firefox 66 (Win 8.1/10)      TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Firefox 100 (Win 10)         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 IE 6 XP                      No connection
 IE 8 Win 7                   No connection
 IE 8 XP                      No connection
 IE 11 Win 7                  TLSv1.2   DHE-RSA-AES128-GCM-SHA256         4096 bit DH
 IE 11 Win 8.1                TLSv1.2   DHE-RSA-AES128-GCM-SHA256         4096 bit DH
 IE 11 Win Phone 8.1          No connection
 IE 11 Win 10                 TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Edge 15 Win 10               TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 Edge 101 Win 10 21H2         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 12.1 (iOS 12.2)       TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 13.0 (macOS 10.14.6)  TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 15.4 (macOS 12.3.1)   TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
```

```
(X25519)
 Java 7u25                   No connection
 Java 8u161                  TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Java 11.0.2 (OpenJDK)       TLSv1.3   TLS_AES_256_GCM_SHA384            256 bit ECDH
(P-256)
 Java 17.0.3 (OpenJDK)       TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 go 1.17.8                   TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 LibreSSL 2.8.3 (Apple)      TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 OpenSSL 1.0.2e              TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 OpenSSL 1.1.0l (Debian)     TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 OpenSSL 1.1.1d (Debian)     TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 OpenSSL 3.0.3 (git)         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Apple Mail (16.0)           TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Thunderbird (91.9)          TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)


 Rating (experimental)

 Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from
2020-01-30)
 Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rat-
ing-Guide
 Protocol Support (weighted)  100 (30)
 Key Exchange     (weighted)  90 (27)
 Cipher Strength  (weighted)  90 (36)
 Final Score                  93
 Overall Grade                A+

 Done 2024-11-19 15:04:45 [  74s] -->> 80.158.47.21:443 (tuv-pentest.evermood.com) <<--
```

A.4 Detailed TLS Scan Results (Retest)

The following is scan data for each system.

A.4.1 tuv-pentest.evermood.com (80.158.47.21) Port 443

```
## Scan started as: "testssl --log tuv-pentest.evermood.com"
## at kali:/usr/bin/openssl
## version testssl: 3.2rc4  from
## version openssl: "3.4.0" from "Jan  6 18:01:42 2025")

 Start 2025-02-20 15:38:57               -->> 80.158.47.21:443 (tuv-pen-
test.evermood.com) <<--

 rDNS (80.158.47.21):    ecs-80-158-47-21.reverse.open-telekom-cloud.com.
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
```

```
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            not offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits
------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 x9e     DHE-RSA-AES128-GCM-SHA256         DH 4096    AESGCM      128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 x9f     DHE-RSA-AES256-GCM-SHA384         DH 4096    AESGCM      256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.3 (server order)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256

 Has server cipher order?     yes (OK) -- TLS 1.3 and below


 Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES,
RC4

 FS is offered (OK)           TLS_AES_256_GCM_SHA384
                              ECDHE-RSA-AES256-GCM-SHA384
                              DHE-RSA-AES256-GCM-SHA384 TLS_AES_128_GCM_SHA256
                              ECDHE-RSA-AES128-GCM-SHA256
                              DHE-RSA-AES128-GCM-SHA256
 Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519 X448
 Finite field group:          ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192
 TLS 1.2 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384
                              RSA-PSS-RSAE+SHA512 RSA+SHA256 RSA+SHA384
                              RSA+SHA512 RSA+SHA224
 TLS 1.3 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384
                              RSA-PSS-RSAE+SHA512
```

```
 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281" "server name/#0"
                              "EC point formats/#11" "supported versions/#43"
                              "key share/#51" "max fragment length/#1"
                              "application layer protocol negotiation/#16"
                              "extended master secret/#23"
 Session Ticket RFC 5077 hint no -- no lifetime advertised
 SSL Session ID support       yes
 Session Resumption           Tickets no, ID: no
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      none
 Client Authentication        none
 Signature Algorithm          SHA256 with RSA
 Server key size              RSA 2048 bits (exponent is 65537)
 Server key usage             Digital Signature, Key Encipherment
 Server extended key usage    TLS Web Server Authentication, TLS Web Client Authentica-
tion
 Serial                       046AE33BB7A34984C5B7AC835BF6EC8B1F4A (OK: length 18)
 Fingerprints                 SHA1 77641F440C9D6DEEF33322400EB0E1F127889721
                              SHA256 AD53CB7E3D0135106BA084374154C5AB-
B47D9CB2F53D76B24DFE09E58E93F824
 Common Name (CN)             *.evermood.com  (request w/o SNI didn't succeed)
 subjectAltName (SAN)         *.evermood.com
 Trust (hostname)             Ok via SAN wildcard and CN wildcard (SNI mandatory)
                              wildcard certificate could be problematic, see other
hosts at
                              https://search.censys.io/search?
resource=hosts&virtual_hosts=INCLUDE&q=AD53CB7E3D0135106BA084374154C5ABB47D9CB2F53D76B2
4DFE09E58E93F824
 Chain of trust               Ok
 EV cert (experimental)       no
 Certificate Validity (UTC)   34 >= 30 days (2024-12-27 08:57 --> 2025-03-27 08:57)
 ETS/"eTLS", visibility info  not present
 Certificate Revocation List  --
 OCSP URI                     http://r11.o.lencr.org
 OCSP stapling                not offered
 OCSP must staple extension   --
 DNS CAA RR (experimental)    available - please check for match with "Issuer" below
                              issue=letsencrypt.org, issuewild=;
 Certificate Transparency     yes (certificate extension)
 Certificates provided        2
 Issuer                       R11 (Let's Encrypt from US)
 Intermediate cert validity   #1: ok > 40 days (2027-03-12 23:59). R11 <-- ISRG Root X1
 Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code             200 OK
 HTTP clock skew              -1 sec from localtime
 Strict Transport Security    365 days=31536000 s, includeSubDomains
 Public Key Pinning           --
 Server banner                (no "Server" line in header, interesting!)
 Application banner           --
 Cookie(s)                    2 issued: 2/2 secure, 2/2 HttpOnly
 Security headers             X-Frame-Options: SAMEORIGIN
                              X-Content-Type-Options: nosniff
                              Content-Security-Policy: default-src 'self'
                                https:; script-src 'self' https: blob:
                                'nonce-/6KjZDIBMsGxEE7lqKkIGQ==';  style-src
                                'self' https: 'unsafe-inline'; font-src 'self'
                                https: data:; object-src 'none'; connect-src
```

```
                                'self' https: wss: data: https://*.3qsdn.com
                                https://evermood-server-app-data-production.obs.eu-
de.otc.t-systems.com;
                                edia-src 'self' https: blob:
                                https://*.3qsdn.com
                                https://evermood-server-app-data-production.obs.eu-
de.otc.t-systems.com;
                                mg-src 'self' https: data:
                                https://evermood-server-app-data-production.obs.eu-
de.otc.t-systems.com
                              Permissions-Policy: geolocation=(), camera=(),
                                microphone=(), payment=(), display-capture=()
                              Cross-Origin-Opener-Policy: unsafe-none
                              Cross-Origin-Resource-Policy: cross-origin
                              Cross-Origin-Embedder-Policy: unsafe-none
                              X-XSS-Protection: 0
                              Permissions-Policy: geolocation=(), camera=(),
                                microphone=(), payment=(), display-capture=()
                              Referrer-Policy: strict-origin-when-cross-origin
                              Cache-Control: no-store
                              Pragma: no-cache
 Reverse Proxy banner         --


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)               not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                      not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment. not vulnerable (OK), no session ticket
extension
 ROBOT                                    Server does not support any cipher suites
that use RSA key transport
 Secure Renegotiation (RFC 5746)          supported (OK)
 Secure Client-Initiated Renegotiation    not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)               not vulnerable (OK)
 BREACH (CVE-2013-3587)                   potentially NOT ok, "gzip" HTTP compression
detected. - only supplied "/" tested
                                          Can be ignored for static pages or if no
secrets in the page
 POODLE, SSL (CVE-2014-3566)              not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)             No fallback possible (OK), no protocol below
TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)   not vulnerable (OK)
 FREAK (CVE-2015-0204)                    not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)     not vulnerable on this host and port (OK)
                                          make sure you don't use this certificate
elsewhere with SSLv2 enabled services, see
                                          https://search.censys.io/search?
resource=hosts&virtual_hosts=INCLUDE&q=AD53CB7E3D0135106BA084374154C5ABB47D9CB2F53D76B2
4DFE09E58E93F824
 LOGJAM (CVE-2015-4000), experimental     not vulnerable (OK): no DH EXPORT ciphers,
no common prime detected
 BEAST (CVE-2011-3389)                    not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental    not vulnerable (OK)
 Winshock (CVE-2014-6321), experimental   not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)       no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward
Secrecy
------------------------------------------------------------------------------------
---------
```

```
 Android 6.0                TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Android 7.0 (native)       TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Android 8.1 (native)       TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 Android 9.0 (native)       TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 10.0 (native)      TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 11 (native)        TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Android 12 (native)        TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Chrome 79 (Win 10)         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Chrome 101 (Win 10)        TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Firefox 66 (Win 8.1/10)    TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Firefox 100 (Win 10)       TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 IE 6 XP                    No connection
 IE 8 Win 7                 No connection
 IE 8 XP                    No connection
 IE 11 Win 7                TLSv1.2   DHE-RSA-AES128-GCM-SHA256         4096 bit DH
 IE 11 Win 8.1              TLSv1.2   DHE-RSA-AES128-GCM-SHA256         4096 bit DH
 IE 11 Win Phone 8.1        No connection
 IE 11 Win 10               TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Edge 15 Win 10             TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 Edge 101 Win 10 21H2       TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 12.1 (iOS 12.2)     TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 13.0 (macOS 10.14.6) TLSv1.3  TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Safari 15.4 (macOS 12.3.1) TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Java 7u25                  No connection
 Java 8u161                 TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Java 11.0.2 (OpenJDK)      TLSv1.3   TLS_AES_256_GCM_SHA384            256 bit ECDH
(P-256)
 Java 17.0.3 (OpenJDK)      TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 go 1.17.8                  TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 LibreSSL 2.8.3 (Apple)     TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 OpenSSL 1.0.2e             TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 OpenSSL 1.1.0l (Debian)    TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       253 bit ECDH
(X25519)
 OpenSSL 1.1.1d (Debian)    TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 OpenSSL 3.0.3 (git)        TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
 Apple Mail (16.0)          TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256       256 bit ECDH
(P-256)
 Thunderbird (91.9)         TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH
(X25519)
```

```
 Rating (experimental)

 Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from
2020-01-30)
 Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rat-
ing-Guide
 Protocol Support (weighted)  100 (30)
 Key Exchange     (weighted)  90 (27)
 Cipher Strength  (weighted)  90 (36)
 Final Score                  93
 Overall Grade                A+

 Done 2025-02-20 15:40:17 [  87s] -->> 80.158.47.21:443 (tuv-pentest.evermood.com) <<--
```