Security requirement

Load Balancer as Web Server

Deutsche Telekom Group

Version	4.5
Date	Dec 1, 2023
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.59	Security requirement

Version	State	Status
4.5	Dec 1, 2023	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Dec 1, 2023 - Nov 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary

This security document has been prepared based on the general security policies of the Group. It defines the requirements for securely configurating of load balancers used as web servers. The requirements described in this document must be met to ensure that the web server functionality of the load balancer cannot be easily misused by competent attackers.

Table of Contents

1. Introduction 4
2. Load Balancer Software 5
3. Load Balancer Configuration 7
4. HTTPS 9
5. Logging 12

1. Introduction

This security document has been prepared based on the general security policies of the Group. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes.
When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

Comment on the term "**web server**":
A load balancer does not implement the full functionality of a web server, but basically the functionality of a reverse HTTP(S) proxy. Therefore the load balancer can replace a web server only if merely the functionality of a proxy is required.

2. Load Balancer Software

Req 1	Software and hardware of the system must be covered by security vulnerability support from the supplier.

Only software and hardware products for which there is security vulnerability support by the supplier may be used in a system.

Such support must include that the supplier
- continuously monitors and analyzes the product for whether it has been affected by security vulnerabilities,
- informs immediately about the type, severity and exploitability of vulnerabilities discovered in the product
- timely provides product updates or effective workarounds to remedy the vulnerabilities.

The security vulnerability support must be in place for the entire period in which the affected product remains in use.

Support phases with limited scope of services
Many suppliers optionally offer time-extended support for their products, which goes beyond the support phase intended for the general market, but is often associated with limitations. Some suppliers define their support fundamentally in increments, which may include limitations even during the final phase before the absolute end date of regular support.
If a product is used within support phases that are subject to limitations, it must be explicitly ensured that these restrictions do not affect the availability of security vulnerability support.

Open Source Software and Hardware
Open Source products are often developed by free organizations or communities; accordingly, contractually agreed security vulnerability support may not be available. In principle, it must also be ensured here that the organization/community (or a third party officially commissioned by them) operates a comprehensive security vulnerability management for the affected product, which meets the above-mentioned criteria and is considered to be reliably established.

Motivation: Hardware and software products for which there is no comprehensive security vulnerability support from the supplier pose a risk. This means that a product is not adequately checked to determine whether it is affected by further developed forms of attack or newly discovered vulnerabilities in technical implementations. Likewise, if there are existing security vulnerabilities in a product, no improvements (e.g. updates, patches) are provided. This results in a system whose weak points cannot be remedied, so that they remain exploitable by an attacker in order to compromise the system or to adversely affect it.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.01-1/7.0

Req 2	Known vulnerabilities in the software or hardware of the system must be fixed or protected against misuse.

Known vulnerabilities in software and hardware components must be fixed by installing available system updates from the supplier (e.g. patches, updates/upgrades). Alternatively, the use of workarounds (acute solutions that do not fix the vulnerability, but effectively prevent exploitation) is permissible. Workarounds should only be used temporarily and should be replaced by a regular system update as soon as possible in order to completely close the vulnerabilities.

Components that contain known, unrecoverable vulnerabilities must not be used in a system.

The treatment of newly discovered vulnerabilities must also be continuously ensured for the entire deployment phase of the system and implemented in the continuous operating processes of security patch management.

Motivation: The use of components without fixing contained vulnerabilities significantly increases the risk of a successful compromise. The attacker is additionally favored by the fact that, as a rule, not only detailed information on vulnerabilities that have already become known is openly available, but often also already adapted attack tools that facilitate active exploitation.

Implementation example: Following the initial installation of an operating system from an official installation medium, all currently available patches and security updates are installed.

Additional information:
The primary sources of known vulnerabilities in software/hardware are lists in the release notes as well as the security advisories from the official reporting channels of the supplier or independent CERTs. In particular, the reporting channels are sensibly integrated into continuous processes of security patch management for a system, so that newly discovered vulnerabilities can be registered promptly and led into operational remedial measures.
As a complementary measure to the detection of potentially still contained types of vulnerabilities that have in principle already become known, targeted vulnerability investigations of the system can be carried out. Particularly specialized tools such as automated vulnerability scanners are suitable for this purpose. Examples include: Tenable Nessus, Qualys Scanner Appliance.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.01-10/7.0

3. Load Balancer Configuration

Req 3	The web server service must be bound only to interfaces, which are necessary to connect the service.

In most cases the web server service needs to be bound only to one interface.

Motivation: The more interfaces provide access to the web server, the higher is the attack risk.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.03-5/6.0

Req 4	If the load balancer supports an HTTP compliancy check, then it must reject HTTP requests, that do not comply with appropriate protocol specifications.

HTTP requests must comply with RFC2616. An HTTP request, for example, containing an incorrect content length header must be rejected with an appropriate HTTP status code.
Many load balancers support HTTP compliancy check, e.g. by "Strict HTTP inspection".

Motivation: Any request that does not satisfy the RFC specification could indicate an attempted attack.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.59-4/4.5

Req 5	HTTP methods that are not required must be deactivated.

The TRACE/TRACK method must not be used by a productive web server. Standard requests to web servers only use GET and POST. If other methods are required, they must be processed securely.

Motivation: HTTP TRACE could be misused by an attacker. This method allows for debugging and trace analysis of connections between the client and the web server. Other HTTP methods could also be used to obtain information about the server, or they could be directly misused by an attacker.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.03-6/6.0

Req 6 The server string in the HTTP header must be replaced.

The HTTP header must not include information on the version of the load balancer and the modules/add-ons used.

Motivation: Any information about the software could allow conclusions to be drawn about security vulnerabilities. If, for example, the server string is "Server: Apache/2.4.1 (Unix)", then an attacker could look specifically for vulnerabilities of this version.

Implementation example: Change the configuration to deliver

```
Server: Webserver
```

as HTTP header.

For this requirement the following threats are relevant:

- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.59-6/4.5

Req 7 Long runtimes of HTTP requests must be prevented.

The configuration of timeouts, which control the response to HTTP requests, must prevent long runtimes. A request to the web server usually doesn't need more than 10 seconds.
The technical options may differ for different load balancer products.

Motivation: The load balancer performance can be reduced significantly by long runtimes of HTTP requests - up to a denial-of-service. This can be misused for an attack (example: Slowloris).

For this requirement the following threats are relevant:

- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.59-7/4.5

Req 8 The load balancer must protect itself and downstream systems against attacks and faulty requests.

Load balancers provide several configuration options as protection measures, e.g.

- Limit the length of HTTP requests
- Activate "Slow Start"
- Set "maximum connections per real server"
- Protect SynFlood

The specific configuration measures depend on the options of the load balancer (see the documentation of the vendor) and the requirements of the application behind the load balancer.

Motivation: Attacks and faulty requests should be recognised and repelled as early as possible.

For this requirement the following threats are relevant:

- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.59-8/4.5

4. HTTPS

Req 9	For encryption with HTTPS the TLS protocol in version 1.2 or higher must be used.

SSL and TLS 1.0/1.1 must be considered outdated and thus may not be activated or must be deactivated, respectively. TLS in version 1.2 provides a sufficient protocol security and also offers Authenticated Encryption Associated Data (AEAD) encryption schemes.

Motivation: The current versions of TLS fix previous known security vulnerabilites and attack surfaces on the TLS protocol handshake.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-21/6.0

Req 10	The web server must be configured in such a way that the use of the latest version of the TLS protocol is enabled.

Motivation: The latest version of the protocol offers the best possible protection and contains fixes to known vulnerabilities in previous versions of the protocol.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-22/6.0

Req 11	The TLS configuration must use secure cipher suites.

Acceptable cipher suites may only use the following algorithms:

Server/Client Authentication & Key Agreement	**Encryption**	**Message Authentication & Integrity (MAC)**
ECDHE_ECDSA ECDHE_RSA DHE_DSS[1] DHE_RSA[1]	AES_128_CBC AES_128_GCM AES_128_CCM AES_192_CBC AES_192_GCM AES_192_CCM AES_256_CBC AES_256_GCM AES_256_CCM CHACHA20_POLY1305	SHA256 SHA384 SHA512 SHA-3-256 SHA-3-384 SHA-3-512

[1]min. 4096-bit Parameter

TLS 1.3 explicitly specifies the usage of only DHE and ECDHE for server/client authentication and key agreement. Thus TLS 1.3 cipher suite notation does not contain an indication in this regard.

By fulfilling this requirement the Perfect Forward Secrecy (PFS) property in the TLS/SSL implementation will be achieved.

Motivation: Cipher suites known to be unsecure do not offer sufficient protection.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-23/6.0

Req 12	The TLS configuration must provide that the cipher suite considered most secure is being chosen with highest priority.

A cipher suite contains the definition of four algoritthms. These are used for key exchange, authentication, encryption and as a hash function. General guidelines for the prioritization are

- For the key exchange the Diffie-Hellman method must be used because it offers perfect forward secrecy. Cipher suites using the Diffie-Hellman method may be identified by the strings DHE or ECDHE. ECDHE has higher priority than DHE.
- For encryption the Advanced Encryption Standard (AES) with a key length as big as possible has to be used
- As a hash function SHA-2 or SHA-3 has to be used. These functions usually may be identified by the string SHA or SHA-3**followed by a number**(256, 384 or 512). Warning: if the string SHA is not followed by a number this identifies the SHA-1 function which is significantly less secure.

Motivation: When a TLS connection is being established a cipher suite is selected based on the cipher suites available both on client and on server side. In order to ensure a high compatibility to all kinds of client systems the web server must not only allow for the cipher suites considered most secure. To make sure that nevertheless for each client the best possible cipher suite is selected and thus the connection is best protected the configuration must contain an according prioritization.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-24/6.0

Req 13	Certificates must be issued by a certification authority whose certificates are recognized by the commonly used web browsers.

For critical applications that can be used via the Internet, use of an extended validation certificate (EV certificate) is recommended.

Motivation: Only if the certificate authority (CA) is contained in the CA list of the browser being used the browser can verify the authenticity of the server.or web application
Stricter issuing criteria apply to EV certificates. If an EV certificate is used, this is visualized in the browser. Even if EV

certificates do not improve security, their use increases the trustworthiness of the server for the user.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.03-25/6.0

Req 14	Certificates must lose their validity after a maximum of 1 year.

In the case of certificates of an internal CA, in particular for machine interfaces, the period may be extended to a maximum of 3 years.

Motivation: The methods used for analysing and breaking cryptographic processes are improved continuously. Therefore the security of the certificates can be ensured for a limited period only. But, according to a general estimation, the security of the certificates is ensured for the required validity period of one year, if an appropriate key length is used.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-26/6.0

Req 15	Certificates must have a key length of at least 3072 bits when using RSA or 256 bits when using ECC.

Remarks on DSA and RSA certificates:
For DSA and RSA, key lengths smaller than 3000 bits may only be used in legacy systems [BSI TR-02102-1] until the end of 2025 and
should be substituted at the next opportunity. Because of the better performance, elliptic curve (EC-DSA) certificates shall be preferred (if supported and technically doable).
RSA-PKCS#1 v1.5 may only be used in legacy systems and should be (if feasible) substituted at the earliest opportunity [BSI TR-02102-1].

References:
[BSI TR-02102-1] Bundesamt für Sicherheit in der Informationstechnik: Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1, Version 2022-01, 28.01.2022

Motivation: In order to guarantee the security of certificates over the validity period, the cryptographic keys must have an appropriate length. According to a general estimation, a key length of 3072 bits provides sufficient protection for the next years. For ECC algorithms, shorter key lengths already provide the same level of security.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.03-27/6.0

5. Logging

Req 16	Applicable retention and deletion periods must be observed for security-relevant logging data that is recorded locally.

From an IT security perspective, local storage of security-relevant logging data on a system is not mandatory. Since the local storage can be damaged in the event of system malfunctions or manipulated by a successful attacker, it can only be used to a limited extent for security-related or forensic analyses. Accordingly, it is relevant for IT security that logging data is forwarded to a separate log server.

Local storage can nevertheless take place; for example, if local storage is initially indispensable when generating the logging data due to technical processes or if there are justified operational interests in also keeping logging data available locally.

The following basic rules must be taken into account when storing logging data locally:

- Security-related logging data must be retained for a period of 90 days.
  (*This requirement only applies if no additional forwarding to a separate log server is implemented on the system and the logging data is therefore only recorded locally.*)
- After 90 days, stored logging data must be deleted immediately.

Deviances

Different retention periods and deletion periods may exist due to legal or regulatory requirements (especially in connection with personal data) or may be defined by contractual agreements. In these cases, the applicable periods must be agreed individually with a Project Security Manager (PSM) / Data Privacy Advisor (DPA) or are specified by them.

Motivation: Logging data is an immensely important IT security tool for preventing, detecting and clearing up system faults, security and data privacy incidents. On the other hand, the recording of logging data, like any other data processing, is also subject to legal and regulatory requirements. Accordingly, guidelines must be adhered to that reconcile the two.

Implementation example: Taking into account the current legal situation and applicable data privacy regulations, the following deletion periods for locally stored security-relevant logging data are implemented on an exemplary telecommunications system:

- Standard System Logs: Deletion after 90 days at the latest
- Logging of public IP addresses: Deletion (or anonymization) after 7 days at the latest
- Logging of the assignment of dynamic public IP addresses by the telecommunication solution: Deletion after 7 days at the latest
- Logging of non-billing-relevant call detail records: Deletion after 7 days at the latest
- Logging of the content of e-mail and SMS: Deletion after 24 hours at the latest
- Logging of the domain queries handled by the DNS server of the telecommunications solution: Deletion after 24 hours at the latest

For this requirement the following threats are relevant:

- Unauthorized access or tapping of data
- Denial of executed activities
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.01-34/7.0

Req 17	For security-relevant logging data that is forwarded to the separate log server, compliance with the applicable retention and deletion periods must be ensured.

The following basic rules must be taken into account:

- security-related logging data must be retained for a period of 90 days on the separate log server.
- after 90 days, stored logging data must be deleted immediately on the separate log server.

Deviances

Different retention periods and deletion periods may exist due to legal or regulatory requirements (especially in connection with personal data) or may be defined by contractual agreements. In these cases, the applicable periods must be agreed individually with a Project Security Manager (PSM) / Data Privacy Advisor (DSB) or are specified by them.

Log server under the responsibility of a third party

If the selected separate log server is not within the same operational responsibility as the source system of the loggin data, it must be ensured that the responsible operator of the log server is aware of the valid parameters for the logging data to be received and that they are adhered to in accordance with the regulations mentioned here.

Motivation: Logging data is an immensely important IT security tool for preventing, detecting and clearing up system faults, security and data privacy incidents. On the other hand, the recording of logging data, like any other data processing, is also subject to legal and regulatory requirements. Accordingly, guidelines must be adhered to that reconcile the two.

Implementation example: Taking into account the current legal situation and applicable data privacy regulations, the following deletion periods for forwarded security-relevant logging data from an exemplary telecommunications system are implemented on the separate log server:

- Standard System Logs: Deletion after 90 days at the latest
- Logging of public IP addresses: Deletion (or anonymization) after 7 days at the latest
- Logging of the assignment of dynamic public IP addresses by the telecommunication solution: Deletion after 7 days at the latest
- Logging of non-billing-relevant call detail records: Deletion after 7 days at the latest
- Logging of the content of e-mail and SMS: Deletion after 24 hours at the latest
- Logging of the domain queries handled by the DNS server of the telecommunications solution: Deletion after 24 hours at the latest

For this requirement the following threats are relevant:

- Unauthorized access or tapping of data
- Denial of executed activities
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.01-36/7.0