ipban.de

Automatisierter Sicherheitsscan – ein Dienst der TeleNoise GmbH

Sicherheitsbericht

Gesamtübersicht aller Ziele – anonymisiertes Beispiel

Kunde	Musterfirma GmbH (K1234)
Ziele	www.musterfirma.de, mail.musterfirma.de
Gesamtbewertung	**D** – Kritische Befunde – sofort handeln und einen IT-Dienstleister hinzuziehen.
Offene Befunde	28
Erstellt am	26.11.2026, 10:04

Vertraulich – dieser Bericht enthält Informationen über Schwachstellen Ihrer Systeme. Geben Sie ihn nur an Personen weiter, die mit der Behebung betraut sind.

Beispielbericht

Dieser Bericht beruht auf einem echten Scan. Firmenname, Kundennummer, Domains, IP-Adressen und Zertifikatsdaten wurden durch Platzhalter ersetzt (Musterfirma GmbH, musterfirma.de, IP-Adressen aus den Dokumentationsbereichen). Die Befunde selbst sind unverändert.

Zusammenfassung

D

Gesamtbewertung D

Kritische Befunde – sofort handeln und einen IT-Dienstleister hinzuziehen.

Die Gesamtbewertung ist die schlechteste Bewertung aller Ziele – ein einziges verwundbares System genügt für einen erfolgreichen Angriff.

2	0	19	7
Kritisch	Hoch	Mittel	Niedrig

Kritische Befunde (CVSS 9,0 bis 10,0)

Ein kritischer Befund bedeutet in der Regel, dass ein Angreifer Ihr System ohne Zugangsdaten übernehmen, Daten stehlen oder verschlüsseln kann. Warten Sie nicht auf den nächsten Monatsscan: Ziehen Sie sofort einen IT-Dienstleister hinzu – zum Beispiel die TeleNoise GmbH unter ticket@telenoise.de. Ist das System nicht zwingend aus dem Internet erreichbar, trennen Sie es bis zur Behebung vom Netz oder sperren Sie den betroffenen Port in der Firewall.

Ziele

ZIEL	BEWERTUNG	LETZTER SCAN	OFFENE BEFUNDE	NÄCHSTER MONATSSCAN
www.musterfirma.de	D	11.11.2026 · Erstscan	2 / 0 / 4 / 4	11.12.2026
mail.musterfirma.de	B	11.11.2026 · Erstscan	0 / 0 / 15 / 3	11.12.2026

Offene Befunde: kritisch / hoch / mittel / niedrig

Überwachung

ZIEL	PRÜFUNG	STATUS	
musterfirma.de	DNS	OK	2 Nameserver · 1 MX · 2 IP
musterfirma.de	Domain	OK	registriert (Ablauf verlängert sich automatisch)
musterfirma.de	E-Mail-Sicherheit	Hinweis	SPF ✓ · DMARC ✓ · DKIM ✓ · keine Blacklist

www.musterfirma.de	SSL-Zertifikat	OK	gültig, noch 72 Tage · Let's Encrypt
www.musterfirma.de	Erreichbarkeit	OK	erreichbar · 15 ms (HTTPS)
mail.musterfirma.de	SSL-Zertifikat	OK	gültig, noch 86 Tage · Let's Encrypt
mail.musterfirma.de	Erreichbarkeit	OK	erreichbar · 11 ms (Ping)

Offene Befunde im Überblick

RISIKO	BEFUND	ZIEL	PORT	CVSS
Kritisch	Operating System (OS) End of Life (EOL) Detection	www.musterfirma.de	general/tcp	10,0
Kritisch	Operating System (OS) End of Life (EOL) Detection	www.musterfirma.de	general/tcp	10,0
Mittel	SSL/TLS: Certificate Expired	mail.musterfirma.de	25/tcp	5,0
Mittel	DNS Cache Snooping Vulnerability (UDP) - Active Check	mail.musterfirma.de	53/udp	5,0
Mittel	DNS Amplification Attacks (UDP) - Active Check	mail.musterfirma.de	53/udp	5,0
Mittel	Check if Mailserver answer to VRFY and EXPN requests	mail.musterfirma.de	25/tcp	5,0
Mittel	SSL/TLS: Certificate Expired	mail.musterfirma.de	587/tcp	5,0
Mittel	SSL/TLS: Certificate Expired	mail.musterfirma.de	465/tcp	5,0
Mittel	SSL/TLS: Certificate Expired	mail.musterfirma.de	8080/tcp	5,0
Mittel	SSL/TLS: Certificate Expired	mail.musterfirma.de	8081/tcp	5,0
Mittel	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	www.musterfirma.de	25/tcp	5,0
Mittel	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	www.musterfirma.de	25/tcp	5,0
Mittel	IMAP Unencrypted Cleartext Login	mail.musterfirma.de	143/tcp	4,8
Mittel	FTP Unencrypted Cleartext Login	mail.musterfirma.de	21/tcp	4,8

Mittel	SMTP Unencrypted Cleartext Login	mail.musterfirma.de	25/tcp	4,8
Mittel	POP3 Unencrypted Cleartext Login	mail.musterfirma.de	110/tcp	4,8
Mittel	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	mail.musterfirma.de	587/tcp	4,3
Mittel	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	mail.musterfirma.de	465/tcp	4,3
Mittel	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	mail.musterfirma.de	25/tcp	4,3
Mittel	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	www.musterfirma.de	25/tcp	4,3
Mittel	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	www.musterfirma.de	25/tcp	4,3
Niedrig	TCP Timestamps Information Disclosure	mail.musterfirma.de	general/tcp	2,6
Niedrig	Weak MAC Algorithm(s) Supported (SSH)	mail.musterfirma.de	2222/tcp	2,6
Niedrig	Weak MAC Algorithm(s) Supported (SSH)	www.musterfirma.de	2222/tcp	2,6
Niedrig	Weak MAC Algorithm(s) Supported (SSH)	www.musterfirma.de	2222/tcp	2,6
Niedrig	TCP Timestamps Information Disclosure	www.musterfirma.de	general/tcp	2,6
Niedrig	ICMP Timestamp Reply Information Disclosure	mail.musterfirma.de	general/icmp	2,1
Niedrig	ICMP Timestamp Reply Information Disclosure	www.musterfirma.de	general/icmp	2,1

So gehen Sie vor

1. Zuerst kritische und hohe Befunde beheben – besonders auf Systemen, die aus dem Internet erreichbar sein müssen.
2. Den Lösungsvorschlag an Ihre IT, Ihren Hoster oder Dienstleister weitergeben. Meist hilft ein Update, das Abschalten eines nicht benötigten Dienstes oder eine Firewall-Regel.
3. Den Befund im Kundenportal als behoben markieren und eine Nachprüfung anfordern – der nächste Scan bestätigt die Behebung.

Hilfe bei der Behebung

Die IT-Spezialisten der TeleNoise GmbH beheben Befunde für Sie – nach Aufwand oder zum Festpreis. Schreiben Sie an ticket@telenoise.de und nennen Sie Ihre Kundennummer.

Hinweis: Automatisierte Scans geben den Stand zum Zeitpunkt der Prüfung wieder und können nicht jede Schwachstelle erkennen. Einzelne Befunde können Fehlalarme sein, z. B. wenn Sicherheitsupdates ohne Versionswechsel eingespielt wurden.

Befunde im Detail

Kritisch

Operating System (OS) End of Life (EOL) Detection

www.musterfirma.de · Port general/tcp · 203.0.113.10 · CVSS 10,0 · Neu

BESCHREIBUNG

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

AUSWIRKUNG

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

NACHWEIS

```
The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:11

Installed version, build or SP: 11

EOL date: 2026-08-31

EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table
```

Lösungsvorschlag

Risiko mindern: Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Note / Important: Please create an override for this result if the target host is a:

- Windows system with Extended Security Updates (ESU)

- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

Kritisch

Operating System (OS) End of Life (EOL) Detection

www.musterfirma.de · Port general/tcp · 2001:db8:10::10 · CVSS 10,0 · Neu

BESCHREIBUNG

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

AUSWIRKUNG

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

NACHWEIS

```
The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:11

Installed version, build or SP: 11

EOL date: 2026-08-31

EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table
```

Lösungsvorschlag

Risiko mindern: Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Note / Important: Please create an override for this result if the target host is a:

- Windows system with Extended Security Updates (ESU)

- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

Mittel

SSL/TLS: Certificate Expired

mail.musterfirma.de · Port 25/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The remote server's SSL/TLS certificate has already expired.

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

NACHWEIS

```
The certificate of the remote service expired on 2026-02-24 07:26:05.

Certificate details:
fingerprint (SHA-1) | 30877432D1026706D7E805DA846A32C3BB81E3C2
fingerprint (SHA-256) | 9B62179273C8EB5BB682575EC87A171AC826A6FCE48478DCB74F21345D2CCE80
issued by | CN=E8,O=Let's Encrypt,C=US
public key algorithm | EC/ECDSA
public key size (bits) | 256
serial | 38A39D5E0853964B50AF03B971722F244F58
signature algorithm | ecdsa-with-SHA384
subject | CN=mail.musterfirma.de
subject alternative names (SAN) | mail.musterfirma.de
valid from | 2025-11-26 07:26:06 UTC
valid until | 2026-02-24 07:26:05 UTC
```

Lösungsvorschlag

Risiko mindern: Replace the SSL/TLS certificate by a new one.

Mittel

DNS Cache Snooping Vulnerability (UDP) - Active Check

mail.musterfirma.de · Port 53/udp · 203.0.113.20 · CVSS 5,0 · Neu

BESCHREIBUNG

The DNS server is prone to a cache snooping vulnerability.

DNS cache snooping is when someone queries a DNS server in
order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby
deduce if the DNS server's owner (or its users) have recently visited a specific site.

This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.

This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.

DNS cache snooping is possible even if the DNS server is not configured to resolve recursively
for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a.
'lame requests').

AUSWIRKUNG

Attackers might gain information about cached DNS records
which might lead to further attacks.

Note: This finding might be an acceptable risk if you:

- trust all clients which can reach the server

- do not allow recursive queries from outside your trusted client network.

NACHWEIS

```
Received (an) answer(s) for a non-recursive query for "example.com".

Result:

198.51.100.7
```

Lösungsvorschlag

Risiko mindern: There are multiple possible mitigation steps depending on
location and functionality needed by the DNS server:

- Disable recursion

- Don't allow public access to DNS Servers doing recursion

- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients

- If the risk is accepted either create an override for this result or configure the 'Private LAN' setting mentioned earlier

Weiterführende Informationen: https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf · https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-server-cache-snooping-attacks · https://kb.isc.org/docs/aa-00509 · https://kb.isc.org/docs/aa-00482

Mittel

DNS Amplification Attacks (UDP) - Active Check

mail.musterfirma.de · Port 53/udp · 203.0.113.20 · CVSS 5,0 · CVE-2006-0987 · Neu

BESCHREIBUNG

A misconfigured Domain Name System (DNS) server can be exploited to participate in a Distributed Denial of Service (DDoS) attack.

A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS) that relies on the use of publicly accessible open recursive DNS servers to overwhelm a victim system with DNS response traffic.

The basic attack technique consists of an attacker sending a DNS name lookup request to an open recursive DNS server with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent instead to the victim. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with little effort. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks.

Note: This finding might be an acceptable risk if you:

- trust all clients which can reach the server

- do not allow recursive queries from outside your trusted client network

NACHWEIS

```
We have sent a DNS request of 17 bytes and received a response of 504 bytes.
```

Lösungsvorschlag

Risiko mindern: There are multiple possible mitigation steps known depending on location and functionality needed by the DNS server:

- Disable recursion

- Don't allow public access to DNS Servers doing recursion

- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached

by untrusted clients

- Re-locate the target host to a private LAN

Note: Please create an override for this result if one of the following applies:

- There are additional access restrictions already in place and the IP of the scanner host is included in the allow / access control list

- The increased risk of this exposure is accepted

Weiterführende Informationen: NVD – CVE-2006-0987 · https://web.archive.org/web/20130510195702/http://www.isotf.org/news/DNS-Amplification-Attacks.pdf · https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks

Mittel

Check if Mailserver answer to VRFY and EXPN requests

mail.musterfirma.de · Port 25/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The Mailserver on this host answers to VRFY and/or EXPN requests.

VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

NACHWEIS

```
'VRFY root' produces the following answer: 252 2.0.0 root
```

Lösungsvorschlag

Workaround anwenden: Disable VRFY and/or EXPN on your Mailserver.

For postfix add 'disable_vrfy_command=yes' in 'main.cf'.

For Sendmail add the option 'O PrivacyOptions=goaway'.

It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Weiterführende Informationen: http://cr.yp.to/smtp/vrfy.html

Mittel

SSL/TLS: Certificate Expired

mail.musterfirma.de · Port 587/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The remote server's SSL/TLS certificate has already expired.

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

NACHWEIS

```
The certificate of the remote service expired on 2026-02-24 07:26:05.

Certificate details:
fingerprint (SHA-1) | 30877432D1026706D7E805DA846A32C3BB81E3C2
fingerprint (SHA-256) | 9B62179273C8EB5BB682575EC87A171AC826A6FCE48478DCB74F21345D2CCE80
issued by | CN=E8,O=Let's Encrypt,C=US
public key algorithm | EC/ECDSA
public key size (bits) | 256
serial | 38A39D5E0853964B50AF03B971722F244F58
signature algorithm | ecdsa-with-SHA384
subject | CN=mail.musterfirma.de
subject alternative names (SAN) | mail.musterfirma.de
valid from | 2025-11-26 07:26:06 UTC
valid until | 2026-02-24 07:26:05 UTC
```

Lösungsvorschlag

Risiko mindern: Replace the SSL/TLS certificate by a new one.

Mittel

SSL/TLS: Certificate Expired

mail.musterfirma.de · Port 465/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The remote server's SSL/TLS certificate has already expired.

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

NACHWEIS

```
The certificate of the remote service expired on 2026-02-24 07:26:05.

Certificate details:
fingerprint (SHA-1) | 30877432D1026706D7E805DA846A32C3BB81E3C2
fingerprint (SHA-256) | 9B62179273C8EB5BB682575EC87A171AC826A6FCE48478DCB74F21345D2CCE80
issued by | CN=E8,O=Let's Encrypt,C=US
public key algorithm | EC/ECDSA
public key size (bits) | 256
serial | 38A39D5E0853964B50AF03B971722F244F58
signature algorithm | ecdsa-with-SHA384
subject | CN=mail.musterfirma.de
subject alternative names (SAN) | mail.musterfirma.de
valid from | 2025-11-26 07:26:06 UTC
valid until | 2026-02-24 07:26:05 UTC
```

Lösungsvorschlag

Risiko mindern: Replace the SSL/TLS certificate by a new one.

Mittel

SSL/TLS: Certificate Expired

mail.musterfirma.de · Port 8080/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The remote server's SSL/TLS certificate has already expired.

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

NACHWEIS

```
The certificate of the remote service expired on 2026-02-24 07:26:05.

Certificate details:
fingerprint (SHA-1) | 30877432D1026706D7E805DA846A32C3BB81E3C2
fingerprint (SHA-256) | 9B62179273C8EB5BB682575EC87A171AC826A6FCE48478DCB74F21345D2CCE80
issued by | CN=E8,O=Let's Encrypt,C=US
public key algorithm | EC/ECDSA
public key size (bits) | 256
serial | 38A39D5E0853964B50AF03B971722F244F58
signature algorithm | ecdsa-with-SHA384
subject | CN=mail.musterfirma.de
subject alternative names (SAN) | mail.musterfirma.de
valid from | 2025-11-26 07:26:06 UTC
valid until | 2026-02-24 07:26:05 UTC
```

Lösungsvorschlag

Risiko mindern: Replace the SSL/TLS certificate by a new one.

Mittel

SSL/TLS: Certificate Expired

mail.musterfirma.de · Port 8081/tcp · 203.0.113.20 · CVSS 5,0 · Offen

BESCHREIBUNG

The remote server's SSL/TLS certificate has already expired.

This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.

NACHWEIS

```
The certificate of the remote service expired on 2026-02-24 07:26:05.

Certificate details:
fingerprint (SHA-1) | 30877432D1026706D7E805DA846A32C3BB81E3C2
fingerprint (SHA-256) | 9B62179273C8EB5BB682575EC87A171AC826A6FCE48478DCB74F21345D2CCE80
issued by | CN=E8,O=Let's Encrypt,C=US
public key algorithm | EC/ECDSA
public key size (bits) | 256
serial | 38A39D5E0853964B50AF03B971722F244F58
signature algorithm | ecdsa-with-SHA384
subject | CN=mail.musterfirma.de
subject alternative names (SAN) | mail.musterfirma.de
valid from | 2025-11-26 07:26:06 UTC
valid until | 2026-02-24 07:26:05 UTC
```

Lösungsvorschlag

Risiko mindern: Replace the SSL/TLS certificate by a new one.

Mittel

SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

www.musterfirma.de · Port 25/tcp · 203.0.113.10 · CVSS 5,0 · CVE-2011-1473, CVE-2011-5094 · Neu

BESCHREIBUNG

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Betroffen: Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

AUSWIRKUNG

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

NACHWEIS

```
The following indicates that the remote SSL/TLS service is affected:

Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an existing / already
established SSL/TLS connection
------------------------------------------------------------
TLSv1.0 | 10
TLSv1.1 | 10
TLSv1.2 | 10
```

Lösungsvorschlag

Update des Herstellers einspielen: Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Weiterführende Informationen: NVD – CVE-2011-1473 · NVD – CVE-2011-5094 · https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ · https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8lU/

Mittel

SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

www.musterfirma.de · Port 25/tcp · 2001:db8:10::10 · CVSS 5,0 · CVE-2011-1473, CVE-2011-5094 · Offen

BESCHREIBUNG

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Betroffen: Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

AUSWIRKUNG

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

NACHWEIS

```
The following indicates that the remote SSL/TLS service is affected:

Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an existing / already
established SSL/TLS connection
------------------------------------------------------------
TLSv1.0 | 10
TLSv1.1 | 10
TLSv1.2 | 10
```

Lösungsvorschlag

Update des Herstellers einspielen: Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Weiterführende Informationen: NVD – CVE-2011-1473 · NVD – CVE-2011-5094 · https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renegotiation-dos/ · https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/

Mittel

IMAP Unencrypted Cleartext Login

mail.musterfirma.de · Port 143/tcp · 203.0.113.20 · CVSS 4,8 · Neu

BESCHREIBUNG

The remote host is running an IMAP daemon that allows cleartext logins over unencrypted connections.

NOTE: Valid credentials needs to given to the settings of 'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.

AUSWIRKUNG

An attacker can uncover user names and passwords by sniffing traffic to the IMAP daemon if a less secure authentication mechanism (eg, LOGIN command, AUTH=PLAIN, AUTH=LOGIN) is used.

NACHWEIS

```
The remote IMAP server accepts logins via the following cleartext authentication mechanisms over unencrypted
connections:

AUTH=LOGIN
AUTH=PLAIN

The remote IMAP server supports the 'STARTTLS' command but isn't enforcing the use of it for the cleartext
authentication mechanisms.
```

Lösungsvorschlag

Risiko mindern: Configure the remote server to always enforce encrypted connections via SSL/TLS with the 'STARTTLS' command.

Weiterführende Informationen: http://www.ietf.org/rfc/rfc2222.txt · http://www.ietf.org/rfc/rfc2595.txt

Mittel

FTP Unencrypted Cleartext Login

mail.musterfirma.de · Port 21/tcp · 203.0.113.20 · CVSS 4,8 · Offen

BESCHREIBUNG

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

AUSWIRKUNG

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

NACHWEIS

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Non-anonymous sessions: 331 User openvasvt OK. Password required
Anonymous sessions:

331 User anonymous OK. Password required

The remote FTP service supports the 'AUTH TLS' command but isn't enforcing the use of it for:

- Non-anonymous sessions
- Anonymous sessions
```

Lösungsvorschlag

Risiko mindern: Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Mittel

SMTP Unencrypted Cleartext Login

mail.musterfirma.de · Port 25/tcp · 203.0.113.20 · CVSS 4,8 · Neu

BESCHREIBUNG

The remote host is running a SMTP server that allows cleartext logins over unencrypted connections.

AUSWIRKUNG

An attacker can uncover login names and passwords by sniffing traffic to the SMTP server.

NACHWEIS

```
The remote SMTP server accepts logins via the following cleartext authentication mechanisms over unencrypted
connections:

PLAIN
LOGIN

The remote SMTP server supports the 'STARTTLS' command but isn't enforcing the use of it for the cleartext
authentication mechanisms.
```

Lösungsvorschlag

Risiko mindern: Enable SMTPS or enforce the connection via the 'STARTTLS' command. Please see the manual of the SMTP server for more information.

Mittel

POP3 Unencrypted Cleartext Login

mail.musterfirma.de · Port 110/tcp · 203.0.113.20 · CVSS 4,8 · Neu

BESCHREIBUNG

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections.

NOTE: Depending on the POP3 server configuration valid credentials needs to be given to the settings of 'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.

AUSWIRKUNG

An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

NACHWEIS

```
The remote POP3 server accepts logins via the following cleartext authentication mechanisms over unencrypted
connections:

USER
SASL PLAIN LOGIN

The remote POP3 server supports the 'STLS' command but isn't enforcing the use of it for the cleartext
authentication mechanisms.
```

Lösungsvorschlag

Risiko mindern: Configure the remote server to always enforce encrypted connections via SSL/TLS with the 'STLS' command.

Weiterführende Informationen: http://www.ietf.org/rfc/rfc2222.txt · http://www.ietf.org/rfc/rfc2595.txt

Mittel

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

mail.musterfirma.de · Port 587/tcp · 203.0.113.20 · CVSS 4,3 · CVE-2011-3389, CVE-2015-0204, CVE-2023-41928, CVE-2024-41270 · · Offen

BESCHREIBUNG

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Betroffen: - All services providing an encrypted communication using the
TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

AUSWIRKUNG

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

NACHWEIS

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and
supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher
Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Lösungsvorschlag

Risiko mindern: It is recommended to disable the deprecated TLSv1.0 and/or

TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Weiterführende Informationen: NVD – CVE-2011-3389 · NVD – CVE-2015-0204 · NVD – CVE-2023-41928

Mittel

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

mail.musterfirma.de · Port 465/tcp · 203.0.113.20 · CVSS 4,3 · CVE-2011-3389, CVE-2015-0204, CVE-2023-41928, CVE-2024-41270 · · Offen

BESCHREIBUNG

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Betroffen: - All services providing an encrypted communication using the
TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

AUSWIRKUNG

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

NACHWEIS

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and
supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher
Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Lösungsvorschlag

Risiko mindern: It is recommended to disable the deprecated TLSv1.0 and/or

TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Weiterführende Informationen: NVD – CVE-2011-3389 · NVD – CVE-2015-0204 · NVD – CVE-2023-41928

Mittel

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

mail.musterfirma.de · Port 25/tcp · 203.0.113.20 · CVSS 4,3 · CVE-2011-3389, CVE-2015-0204, CVE-2023-41928, CVE-2024-41270 · · Offen

BESCHREIBUNG

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Betroffen: - All services providing an encrypted communication using the
TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

AUSWIRKUNG

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

NACHWEIS

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and
supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher
Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Lösungsvorschlag

Risiko mindern: It is recommended to disable the deprecated TLSv1.0 and/or

TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Weiterführende Informationen: NVD – CVE-2011-3389 · NVD – CVE-2015-0204 · NVD – CVE-2023-41928

Mittel

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

www.musterfirma.de · Port 25/tcp · 203.0.113.10 · CVSS 4,3 · CVE-2011-3389, CVE-2015-0204, CVE-2023-41928, CVE-2024-41270 · · Offen

BESCHREIBUNG

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Betroffen: - All services providing an encrypted communication using the
TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

AUSWIRKUNG

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

NACHWEIS

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and
supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher
Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Lösungsvorschlag

Risiko mindern: It is recommended to disable the deprecated TLSv1.0 and/or

TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Weiterführende Informationen: NVD – CVE-2011-3389 · NVD – CVE-2015-0204 · NVD – CVE-2023-41928

Mittel

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

www.musterfirma.de · Port 25/tcp · 2001:db8:10::10 · CVSS 4,3 · CVE-2011-3389, CVE-2015-0204, CVE-2023-41928, · Offen

BESCHREIBUNG

It was possible to detect the usage of the deprecated TLSv1.0
and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic
flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Betroffen: - All services providing an encrypted communication using the
TLSv1.0 and/or TLSv1.1 protocols

- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder

- CVE-2024-41270: Gorush v1.18.4

- CVE-2025-3200: Multiple products from Wiesemann & Theis

AUSWIRKUNG

An attacker might be able to use the known cryptographic flaws to
eavesdrop the connection between clients and the service to get access to sensitive data
transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates
anymore.

NACHWEIS

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and
supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher
Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Lösungsvorschlag

Risiko mindern: It is recommended to disable the deprecated TLSv1.0 and/or

TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Weiterführende Informationen: NVD – CVE-2011-3389 · NVD – CVE-2015-0204 · NVD – CVE-2023-41928

Niedrig

TCP Timestamps Information Disclosure

mail.musterfirma.de · Port general/tcp · 203.0.113.20 · CVSS 2,6 · Neu

BESCHREIBUNG

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Betroffen: TCP implementations that implement RFC1323/RFC7323.

AUSWIRKUNG

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

NACHWEIS

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3266341635
Packet 2: 3605301030
```

Lösungsvorschlag

Risiko mindern: To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Weiterführende Informationen: https://datatracker.ietf.org/doc/html/rfc1323 · https://datatracker.ietf.org/doc/html/rfc7323 · https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 · https://www.fortiguard.com/psirt/FG-IR-16-090

Niedrig

Weak MAC Algorithm(s) Supported (SSH)

mail.musterfirma.de · Port 2222/tcp · 203.0.113.20 · CVSS 2,6 · Neu

BESCHREIBUNG

The remote SSH server is configured to allow / support weak MAC algorithm(s).

NACHWEIS

```
The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com
```

Lösungsvorschlag

Risiko mindern: Disable the reported weak MAC algorithm(s).

Weiterführende Informationen: https://www.rfc-editor.org/rfc/rfc6668 · https://www.rfc-editor.org/rfc/rfc4253#section6.4

Niedrig

Weak MAC Algorithm(s) Supported (SSH)

www.musterfirma.de · Port 2222/tcp · 2001:db8:10::10 · CVSS 2,6 · Neu

BESCHREIBUNG

The remote SSH server is configured to allow / support weak MAC algorithm(s).

NACHWEIS

```
The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com
```

Lösungsvorschlag

Risiko mindern: Disable the reported weak MAC algorithm(s).

Weiterführende Informationen: https://www.rfc-editor.org/rfc/rfc6668 · https://www.rfc-editor.org/rfc/rfc4253#section6.4

Niedrig

Weak MAC Algorithm(s) Supported (SSH)

www.musterfirma.de · Port 2222/tcp · 203.0.113.10 · CVSS 2,6 · Neu

BESCHREIBUNG

The remote SSH server is configured to allow / support weak MAC algorithm(s).

NACHWEIS

```
The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com
```

Lösungsvorschlag

Risiko mindern: Disable the reported weak MAC algorithm(s).

Weiterführende Informationen: https://www.rfc-editor.org/rfc/rfc6668 · https://www.rfc-editor.org/rfc/rfc4253#section6.4

Niedrig

TCP Timestamps Information Disclosure

www.musterfirma.de · Port general/tcp · 203.0.113.10 · CVSS 2,6 · Neu

BESCHREIBUNG

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Betroffen: TCP implementations that implement RFC1323/RFC7323.

AUSWIRKUNG

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

NACHWEIS

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2817363615
Packet 2: 1909666337
```

Lösungsvorschlag

Risiko mindern: To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Weiterführende Informationen: https://datatracker.ietf.org/doc/html/rfc1323 · https://datatracker.ietf.org/doc/html/rfc7323 · https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 · https://www.fortiguard.com/psirt/FG-IR-16-090

Niedrig

ICMP Timestamp Reply Information Disclosure

mail.musterfirma.de · Port general/icmp · 203.0.113.20 · CVSS 2,1 · CVE-1999-0524 · Neu

BESCHREIBUNG

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

AUSWIRKUNG

This information could theoretically be used to exploit weak time-based random number generators in other services.

NACHWEIS

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Lösungsvorschlag

Risiko mindern: Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Weiterführende Informationen: NVD – CVE-1999-0524 · https://datatracker.ietf.org/doc/html/rfc792 · https://datatracker.ietf.org/doc/html/rfc2780

Niedrig

ICMP Timestamp Reply Information Disclosure

www.musterfirma.de · Port general/icmp · 203.0.113.10 · CVSS 2,1 · CVE-1999-0524 · Neu

BESCHREIBUNG

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

AUSWIRKUNG

This information could theoretically be used to exploit weak time-based random number generators in other services.

NACHWEIS

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Lösungsvorschlag

Risiko mindern: Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Weiterführende Informationen: NVD – CVE-1999-0524 · https://datatracker.ietf.org/doc/html/rfc792 · https://datatracker.ietf.org/doc/html/rfc2780