Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240821

Inhaltsverzeichnis

1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

Softwareentwicklung: Schadcode-Attacken auf Jenkins-Server beobachtet

Derzeit nutzen Angreifer eine kritische Lücke im Software-System Jenkins aus. Davon sind auch Instanzen in Deutschland bedroht.

- Link

—

Sicherheitsupdates: Lernplattform Moodle vielfältig angreifbar

Angreifer können unter anderem Schadcode durch Softwareschwachstellen in Moodle schieben. Aktualisierte Versionen sind dagegen abgesichert.

- Link

—

Exploit-Versuch auf Ivanti Virtual Traffic Manager-Lücke

Für die kritische Lücke in Ivantis Virtual Traffic Manager (vTM) wurde ein ein Missbrauchsversuch beobachtet. Alle Patches sind nun verfügbar.

- Link

—

Server mit IBM App Connect Enterprise können nach Attacke abstürzen

IBMs Integrationssoftware App Connect Enterprise ist über eine Sicherheitslücke angreifbar. Ein Sicherheitspatch steht zum Download bereit.

- Link

—

Sicherheitspatch: Angreifer können Dovecot-Mail-Server lahmlegen

Dovecot-IMAP-Server können sich an präparierten E-Mails verschlucken und in einem DoS-Zustand enden.

- Link

—

Jetzt patchen! Schadcode-Attacken auf Solarwinds Web Help Desk beobachtet

Angreifer nutzen derzeit eine kritische Schwachstelle Solarwinds Web Help Desk aus. Ein Sicherheitspatch ist verfügbar, kann aber mitunter für Probleme sorgen.

- Link

—

Serverüberwachung: OpenBMC-Lücke bringt Systeme in Gefahr

Eine kritische Sicherheitslücke in der OpenBMC-Firmware gefährdet Computer. Ein Sicherheitspatch ist verfügbar.

- Link

—

Zoom schützt Anwendungen unter Linux, macOS und Windows vor möglichen Attacken

Es sind wichtige Sicherheitsupdates für unter anderem Zoom Workplace und Rooms Client erschienen.

- Link

—

Sicherheitsupdates F5: Angreifer können unbefugt auf BIG-IP-Appliances zugreifen

Mehrere Sicherheitslücken ermöglichen Attacken auf BIG-IP Next Central Manager und BIG-IP Next SPK.

- Link

—

Solarwinds Web Help Desk: Schadcode kann Host-System infizieren

Eine nun geschlossene kritische Sicherheitslücke bedrohte die Kundensupport-Software Web Help Desk von Solarwinds.

- Link

—

3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-6895	0.921160000	0.989990000	Link
CVE-2023-6553	0.927320000	0.990720000	Link
CVE-2023-5360	0.902780000	0.988760000	Link
CVE-2023-52251	0.946410000	0.992880000	Link
CVE-2023-4966	0.971280000	0.998310000	Link
CVE-2023-49103	0.962110000	0.995620000	Link
CVE-2023-48795	0.965330000	0.996440000	Link
CVE-2023-47246	0.959010000	0.995020000	Link
CVE-2023-46805	0.934240000	0.991450000	Link
CVE-2023-46747	0.972820000	0.998880000	Link
CVE-2023-46604	0.961790000	0.995550000	Link
CVE-2023-4542	0.928310000	0.990810000	Link
CVE-2023-43208	0.972240000	0.998620000	Link
CVE-2023-43177	0.961750000	0.995540000	Link
CVE-2023-42793	0.970220000	0.997890000	Link
CVE-2023-41265	0.911110000	0.989300000	Link
CVE-2023-39143	0.939130000	0.991970000	Link
CVE-2023-38646	0.906610000	0.988990000	Link
CVE-2023-38205	0.953670000	0.994110000	Link
CVE-2023-38203	0.966410000	0.996730000	Link
CVE-2023-38146	0.920720000	0.989950000	Link
CVE-2023-38035	0.974920000	0.999810000	Link
CVE-2023-36845	0.966270000	0.996700000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996580000	Link
CVE-2023-35082	0.966130000	0.996650000	Link
CVE-2023-35078	0.970440000	0.997950000	Link
CVE-2023-34993	0.973130000	0.999020000	Link
CVE-2023-34960	0.928290000	0.990810000	Link
CVE-2023-34634	0.925130000	0.990490000	Link
CVE-2023-34468	0.906650000	0.989000000	Link
CVE-2023-34362	0.971000000	0.998190000	Link
CVE-2023-34039	0.947770000	0.993090000	Link
CVE-2023-3368	0.937150000	0.991700000	Link
CVE-2023-33246	0.972040000	0.998510000	Link
CVE-2023-32315	0.970220000	0.997890000	Link
CVE-2023-30625	0.953800000	0.994130000	Link
CVE-2023-30013	0.962380000	0.995670000	Link
CVE-2023-29300	0.968930000	0.997440000	Link
CVE-2023-29298	0.947600000	0.993060000	Link
CVE-2023-28432	0.911820000	0.989340000	Link
CVE-2023-28343	0.942300000	0.992340000	Link
CVE-2023-28121	0.909500000	0.989160000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.972120000	0.998580000	Link
CVE-2023-27350	0.969720000	0.997720000	Link
CVE-2023-26469	0.956020000	0.994550000	Link
CVE-2023-26360	0.963510000	0.995930000	Link
CVE-2023-26035	0.969020000	0.997460000	Link
CVE-2023-25717	0.954250000	0.994220000	Link
CVE-2023-25194	0.967920000	0.997160000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996040000	Link
CVE-2023-24489	0.973870000	0.999300000	Link
CVE-2023-23752	0.956380000	0.994610000	Link
CVE-2023-23333	0.962300000	0.995650000	Link
CVE-2023-22527	0.968290000	0.997250000	Link
CVE-2023-22518	0.965970000	0.996590000	Link
CVE-2023-22515	0.973250000	0.999060000	Link
CVE-2023-21839	0.955020000	0.994360000	Link
CVE-2023-21554	0.952830000	0.993960000	Link
CVE-2023-20887	0.970670000	0.998040000	Link
CVE-2023-1671	0.964660000	0.996200000	Link
CVE-2023-0669	0.969760000	0.997720000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 20 Aug 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 20 Aug 2024

[NEU] [UNGEPATCHT] [hoch] Autodesk AutoCAD: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Autodesk AutoCAD ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um Administratorrechte zu erlangen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 20 Aug 2024

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 20 Aug 2024

[NEU] [hoch] xwiki: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in xwiki ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- Link

—

Mon, 19 Aug 2024

[NEU] [hoch] Moodle: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Code auszuführen,

bestimmte administrative Aufgaben durchzuführen, Informationen preiszugeben, Daten zu manipulieren, Sicherheitsmechanismen zu umgehen, Cross-Site-Scripting-Angriffe durchzuführen und eine nicht näher spezifizierte Wirkung zu erzielen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/21/2024	[EulerOS Virtualization 2.11.1 : libyaml (EulerOS-SA-2024-2169)]	critical
8/21/2024	[EulerOS Virtualization 2.11.0 : ruby (EulerOS-SA-2024-2199)]	critical
8/20/2024	[Dahua Security (CVE-2024-39950)]	critical
8/21/2024	[EulerOS Virtualization 2.11.1 : curl (EulerOS-SA-2024-2164)]	high
8/21/2024	[EulerOS 2.0 SP12 : kernel (EulerOS-SA-2024-2216)]	high
8/21/2024	[EulerOS 2.0 SP11 : kernel (EulerOS-SA-2024-2206)]	high
8/21/2024	[EulerOS Virtualization 2.11.0 : openssh (EulerOS-SA-2024-2184)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : mod_http2 (EulerOS-SA-2024-2170)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : qemu (EulerOS-SA-2024-2176)]	high
8/21/2024	[EulerOS Virtualization 2.11.0 : less (EulerOS-SA-2024-2180)]	high
8/21/2024	[EulerOS Virtualization 2.11.0 : kernel (EulerOS-SA-2024-2205)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : httpd (EulerOS-SA-2024-2168)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : kernel (EulerOS-SA-2024-2178)]	high

Datum	Schwachstelle	Bewertung
8/21/2024	[EulerOS Virtualization 2.11.1 : libarchive (EulerOS-SA-2024-2156)]	high
8/21/2024	[EulerOS Virtualization 2.11.0 : sssd (EulerOS-SA-2024-2200)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : libxml2 (EulerOS-SA-2024-2158)]	high
8/21/2024	[EulerOS 2.0 SP11 : kernel (EulerOS-SA-2024-2207)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : sssd (EulerOS-SA-2024-2173)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : expat (EulerOS-SA-2024-2166)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : glibc (EulerOS-SA-2024-2154)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : systemd (EulerOS-SA-2024-2162)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : openssh (EulerOS-SA-2024-2159)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : openssl (EulerOS-SA-2024-2160)]	high
8/21/2024	[EulerOS 2.0 SP12 : httpd (EulerOS-SA-2024-2215)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : python-pip (EulerOS-SA-2024-2161)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : less (EulerOS-SA-2024-2155)]	high
8/21/2024	[EulerOS Virtualization 2.11.1 : python3 (EulerOS-SA-2024-2172)]	high
8/20/2024	[EulerOS 2.0 SP12 : kernel (EulerOS-SA-2024-2240)]	high
8/20/2024	[EulerOS Virtualization 2.11.0 : expat (EulerOS-SA-2024-2191)]	high
8/20/2024	[EulerOS 2.0 SP12 : golang (EulerOS-SA-2024-2238)]	high
8/20/2024	[EulerOS Virtualization 2.11.0 : glibc (EulerOS-SA-2024-2179)]	high
8/20/2024	[Dahua Security (CVE-2024-39944)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 20 Aug 2024

Akuvox Smart Intercom/Doorphone Unauthenticated Stream Disclosure

Akuvox Smart Intercom/Doorphone suffers from an unauthenticated live stream disclosure when requesting video.cgi endpoint on port 8080. Many versions are affected.

- Link

—

” “Tue, 20 Aug 2024

Linux Landlock Logic Bug

Linux has an issue where landlock can be disabled thanks to a missing cred_transfer hook.

- Link

—

” “Tue, 20 Aug 2024

Lost and Found Information System 1.0 Cross Site Request Forgery

Lost and Found Information System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Loan Management System 1.0 Cross Site Request Forgery

Loan Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Simple Machines Forum 2.1.4 Code Injection

Simple Machines Forum version 2.1.4 suffers from an authenticated code injection vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Biobook Social Networking Site 1.0 Arbitrary File Upload

Biobook Social Networking Site version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Accounting Journal Management System 1.0 Code Injection

Accounting Journal Management System version 1.0 suffers from a code injection vulnerability.

- Link

—

” “Tue, 20 Aug 2024

ABIC Cardiology Management System 1.0 Cross Site Request Forgery

ABIC Cardiology Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Hospital Management System 1.0 Code Injection

Hospital Management System version 1.0 suffers from a code injection vulnerability.

- Link

—

” “Tue, 20 Aug 2024

Event Registration and Attendance System 1.0 Code Injection

Event Registration and Attendance System version 1.0 suffers from a code injection vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Ewon Cosy+ / Talk2M Remote Access Solution Improper Authentication

During account assignment in the Talk2M platform, a Cosy+ device generates and sends a certificate signing request (CSR) to the back end. This CSR is then signed by the manufacturer and used for OpenVPN authentication by the device afterward. Since the common name (CN) of the certificate is specified by the device and used in order to assign the OpenVPN session to the corresponding Talk2M account, an attacker with root access to a Cosy+ device is able to manipulate the CSR and get correctly signed certificates for foreign devices.

- Link

—

” “Mon, 19 Aug 2024

Dovecot IMAP Server 2.2 / 2.3 Denial Of Service

Dovecot IMAP server versions 2.2 and 2.3 suffer from denial of service and resource exhaustion vulnerabilities.

- Link

—

” “Mon, 19 Aug 2024

Dovecot IMAP Server 2.2 / 2.3 Missing Rate Limiting

Dovecot IMAP server versions 2.2 and 2.3 have an issue where a large number of address headers (From, To, Cc, Bcc, etc.) becomes excessively CPU intensive. With 100k header lines CPU usage is

already 12 seconds, and in a production environment we observed 500k header lines taking 18 minutes to parse. Since this can be triggered by external actors sending emails to a victim, this is a security issue.

- Link

—

” “Mon, 19 Aug 2024

Ewon Cosy+ Hardcoded Key

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. Due to the use of a hardcoded cryptographic key, an attacker is able to decrypt encrypted data and retrieve sensitive information.

- Link

—

” “Mon, 19 Aug 2024

Ewon Cosy+ Command Injection

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. Due to improper neutralization of parameters read from a user-controlled configuration file, an authenticated attacker is able to inject and execute OS commands on the device.

- Link

—

” “Mon, 19 Aug 2024

Ewon Cosy+ Password Disclosure

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. The credentials used for the basic authentication against the web interface of Cosy+ are stored in the cookie ”credentials” after a successful login. An attacker with access to a victim’s browser is able to retrieve the administrative password of Cosy+.

- Link

—

” “Mon, 19 Aug 2024

Ewon Cosy+ Improper Neutralization / Cross Site Scripting

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. If login against the FTP service of the Cosy+ fails, the submitted username is saved in a log. This log is included in the Cosy+ web interface without neutralizing the content. As a result, an unauthenticated attacker is able to inject HTML/JavaScript code via the username of an FTP login attempt.

- Link

—

” “Mon, 19 Aug 2024

Lawyer CMS 1.6 Insecure Settings

Lawyer CMS version 1.6 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Karya Online Shopping Portal 2.0 SQL Injection

Karya Online Shopping Portal version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 19 Aug 2024

JobSeeker CMS 1.5 Insecure Settings

JobSeeker CMS version 1.5 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Jobs Finder System 1.0 SQL Injection

Jobs Finder System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Human Resource Management System 2024 1.0 Insecure Settings

Human Resource Management System 2024 version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Hotel Management System 1.0 Cross Site Request Forgery

Hotel Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Bhojon Restaurant Management System 3.0 Insecure Settings

Bhojon Restaurant Management System version 3.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 19 Aug 2024

Accounting Journal Management System 1.0 Cross Site Request Forgery

Accounting Journal Management System version 1.0 suffers from a cross site request forgery vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Tue, 20 Aug 2024
ZDI-24-1154: Autel MaxiCharger AC Elite Business C50 AppAuthenExchangeRandomNum Stack-Based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Tue, 20 Aug 2024
ZDI-24-1153: Autodesk AutoCAD DWF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Tue, 20 Aug 2024
ZDI-24-1152: Phoenix Contact CHARX SEC-3100 Improper Access Control Authentication Bypass Vulnerability
- Link
—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-19	BVI Electricity Corporation (BVIEC)	[VGB]	Link
2024-08-18	Lagoon	[NCL]	Link
2024-08-17	Bella Vista	[USA]	Link
2024-08-16	Contarina	[ITA]	Link
2024-08-14	Flint	[USA]	Link
2024-08-13	District scolaire indépendant de Gadsden	[USA]	Link
2024-08-13	IPNext	[ARG]	Link
2024-08-12	Benson, Kearley & Associates Insurance Brokers Ltd.	[CAN]	Link
2024-08-11	Université Paris-Saclay	[FRA]	Link
2024-08-11	AutoCanada	[CAN]	Link
2024-08-10	2Park	[NLD]	Link
2024-08-09	Quálitas	[MEX]	Link
2024-08-09	Schlatter Industries AG	[CHE]	Link
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	Link
2024-08-08	Evolution Mining	[AUS]	Link
2024-08-07	Killeen	[USA]	Link
2024-08-06	Nilörn	[SWE]	Link
2024-08-06	Sumter County Sheriff’s Office	[USA]	Link
2024-08-05	La ville de North Miami	[USA]	Link
2024-08-05	McLaren Health Care	[USA]	Link
2024-08-04	RMN-Grand Palais	[FRA]	Link
2024-08-03	Xtrim	[ECU]	Link
2024-08-02	Ihecs	[BEL]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-20	[Codival]	spacebears	Link
2024-08-21	[jpoint.in]	killsec	Link
2024-08-20	[inlighten.net]	ransomhub	Link
2024-08-20	[blowerdempsay.com]	ransomhub	Link
2024-08-20	[atpsassari.it]	helldown	Link
2024-08-20	[Rushlift (lks.net)]	lynx	Link
2024-08-20	[North Georgia Brick]	akira	Link
2024-08-20	[Akkanat Holding]	hunters	Link
2024-08-19	[Percento Technologies Internationa]	medusa	Link
2024-08-19	[OSG.COM]	ransomhub	Link
2024-08-14	[imobesidade.com.br]	ransomhub	Link
2024-08-19	[Waynesboro Nurseries]	rhysida	Link
2024-08-19	[The Transit Authority of Northern Kentucky (TANK)]	akira	Link
2024-08-19	[Khonaysser]	helldown	Link
2024-08-11	[Jangho Group]	ransomhouse	Link
2024-08-19	[Certified Transmission]	meow	Link
2024-08-19	[Bandier]	blacksuit	Link
2024-08-18	[ccsdschools.com]	ransomhub	Link
2024-08-19	[Ferraro Group]	hunters	Link
2024-08-18	[kbo]	helldown	Link
2024-08-18	[Mohawk Valley Cardiology PC]	bianlian	Link
2024-08-18	[PBC Companies]	bianlian	Link
2024-08-17	[Yang Enterprises]	dragonforce	Link
2024-08-17	[Carver Companies]	dragonforce	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-17	[J&J Network Engineering]	dragonforce	Link
2024-08-18	[PER4MANCE]	dragonforce	Link
2024-08-18	[SMK Ingenieurbüro]	dragonforce	Link
2024-08-18	[Cosmetic Dental Group]	trinity	Link
2024-08-17	[TELECO]	stormous	Link
2024-08-17	[peoplewell.com]	darkvault	Link
2024-08-17	[aerworldwide.com]	lockbit3	Link
2024-08-17	[awsag.com]	madliberator	Link
2024-08-17	[www.albynhousing.org.uk]	ransomhub	Link
2024-08-17	[www.lennartsfors.com]	ransomhub	Link
2024-08-17	[www.allanmcneill.co.nz]	ransomhub	Link
2024-08-17	[www.martinswood.herts.sch.uk]	ransomhub	Link
2024-08-17	[www.gmchc.org]	ransomhub	Link
2024-08-17	[www.regentcaravans.com.au]	ransomhub	Link
2024-08-17	[www.netconfig.co.za]	ransomhub	Link
2024-08-17	[www.manotherm.ie]	ransomhub	Link
2024-08-17	[tiendasmacuto.com]	BrainCipher	Link
2024-08-15	[nrcollecties.nl]	ransomhub	Link
2024-08-17	[Zyxel.eu]	helldown	Link
2024-08-10	[www.wmwmeyer.com]	ransomhub	Link
2024-08-16	[www.vinakom.com]	ransomhub	Link
2024-08-16	[Keios Development Consulting]	ciphbit	Link
2024-08-16	[Lennartsfors AB]	meow	Link
2024-08-16	[Rostance Edwards]	meow	Link
2024-08-16	[SuperDrob S.A.]	hunters	Link
2024-08-16	[Sterling Rope]	rhysida	Link
2024-08-16	[www.patelco.org]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-14	[ljglaw.com]	ransomhub	Link
2024-08-16	[Hiesmayr Haustechnik]	qilin	Link
2024-08-15	[www.aaconsultinc.com]	ransomhub	Link
2024-08-16	[promises2kids.org]	qilin	Link
2024-08-16	[BTS Biogas]	hunters	Link
2024-08-15	[www.isnart.it]	ransomhub	Link
2024-08-15	[www.atwoodcherny.com]	ransomhub	Link
2024-08-13	[Mill Creek Lumber]	play	Link
2024-08-14	[Patterson Health Center]	qilin	Link
2024-08-15	[www.prinsotel.com]	qilin	Link
2024-08-15	[Seaway Manufacturing Corp.]	fog	Link
2024-08-15	[FD S.R.L]	ciphbit	Link
2024-08-15	[The Pyle Group]	medusa	Link
2024-08-15	[Zydus Pharmaceuticals]	meow	Link
2024-08-15	[EPS Tech Ltd]	handala	Link
2024-08-15	[MBS Radio]	metaencryptor	Link
2024-08-15	[Liberty Resources]	rhysida	Link
2024-08-15	[megatravel.com.mx]	darkvault	Link
2024-08-14	[startaxi.com]	killsec	Link
2024-08-14	[Boni]	akira	Link
2024-08-14	[The Washington Times]	rhysida	Link
2024-08-12	[Benson Kearley IFG - Insurance Brokers & Financial Advisors]	bianlian	Link
2024-08-14	[Texas Centers for Infectious Disease Associates]	bianlian	Link
2024-08-14	[Thompson Davis & Co]	bianlian	Link
2024-08-14	[police.praca.gov.pl]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-14	[mmtransport.com]	dAn0n	Link
2024-08-14	[Riley Pope & Laney]	cicada3301	Link
2024-08-13	[hugwi.ch]	helldown	Link
2024-08-13	[Forrec]	blacksuit	Link
2024-08-13	[American Contract Systems]	meow	Link
2024-08-13	[Element Food Solutions]	meow	Link
2024-08-13	[Aerotech Solutions]	meow	Link
2024-08-13	[E-Z UP]	meow	Link
2024-08-13	[Safefood]	meow	Link
2024-08-13	[Gaston Fence]	meow	Link
2024-08-13	[Parker Development Company]	play	Link
2024-08-13	[Air International Thermal Systems]	play	Link
2024-08-13	[Adina Design]	play	Link
2024-08-13	[CinemaTech]	play	Link
2024-08-13	[Erie Meats]	play	Link
2024-08-13	[M??? ????k ??????]	play	Link
2024-08-13	[SCHLATTNER.de]	helldown	Link
2024-08-13	[deganis.fr]	helldown	Link
2024-08-13	[The White Center Community Development Association]	rhysida	Link
2024-08-13	[lenmed.co.za]	darkvault	Link
2024-08-13	[gpf.org.za]	darkvault	Link
2024-08-13	[Banner and Associates]	trinity	Link
2024-08-13	[Southwest Family Medicine Associates]	bianlian	Link
2024-08-13	[glazkov.co.il]	darkvault	Link
2024-08-05	[XPERT Business Solutions GmbH]	helldown	Link
2024-08-05	[MyFreightWorld]	helldown	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-09	[cbmm.org]	helldown	Link
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	Link
2024-08-11	[briju.pl]	helldown	Link
2024-08-11	[vindix.pl]	helldown	Link
2024-08-11	[Albatros S.r.l.]	helldown	Link
2024-08-12	[NetOne]	hunters	Link
2024-08-12	[fabamaq.com]	BrainCipher	Link
2024-08-12	[cyceron.fr]	BrainCipher	Link
2024-08-12	[bedford.k12.oh.us]	ransomhub	Link
2024-08-12	[Warwick Hotels and Resorts]	lynx	Link
2024-08-12	[VVS-Eksperten]	cicada3301	Link
2024-08-12	[Brookshire Dental]	qilin	Link
2024-08-07	[Alvan Blanch Development]	lynx	Link
2024-08-11	[parkerdevco.com]	dispossessor	Link
2024-08-11	[naturalcuriosities.com]	ransomhub	Link
2024-08-11	[TelPro]	play	Link
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	Link
2024-08-11	[Amco Metal Industrial Corporation]	qilin	Link
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	Link
2024-08-11	[Moser Wealth Advisors]	rhysida	Link
2024-08-09	[alliuminteriors.co.nz]	ransomhub	Link
2024-08-11	[robertshvac.com]	abyss	Link
2024-08-11	[dmmerch.com]	lockbit3	Link
2024-08-11	[luisoliveras.com]	lockbit3	Link
2024-08-11	[legacycpas.com]	lockbit3	Link
2024-08-11	[allweatheraa.com]	lockbit3	Link
2024-08-11	[soprema.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-11	[exol-lubricants.com]	lockbit3	Link
2024-08-11	[fremontschools.net]	lockbit3	Link
2024-08-11	[acdcexpress.com]	lockbit3	Link
2024-08-11	[clinicatezza.com.pe]	lockbit3	Link
2024-08-11	[divaris.com]	lockbit3	Link
2024-08-11	[sullivansteelservice.com]	lockbit3	Link
2024-08-11	[johnllowery.com]	lockbit3	Link
2024-08-11	[qespavements.com]	lockbit3	Link
2024-08-11	[emanic.net]	lockbit3	Link
2024-08-11	[Hanon Systems]	hunters	Link
2024-08-10	[kronospublic.com]	lockbit3	Link
2024-08-10	[Brontoo Technology Solutions]	ransomexx	Link
2024-08-07	[Cydcor]	dragonforce	Link
2024-08-09	[Credible Group]	play	Link
2024-08-09	[Nilorngruppen AB]	play	Link
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	Link
2024-08-09	[Anniversary Holding Company]	bianlian	Link
2024-08-09	[GCA Global Cargo Alliance]	bianlian	Link
2024-08-09	[Majestic Metals]	bianlian	Link
2024-08-09	[dhcgrp.com]	ransomhub	Link
2024-08-05	[Boombah Inc.]	incransom	Link
2024-08-09	[www.dunnsolutions.com]	dAn0n	Link
2024-08-09	[Sumter County Sheriff]	rhysida	Link
2024-08-06	[pierrediamonds.com.au]	ransomhub	Link
2024-08-08	[golfoy.com]	ransomhub	Link
2024-08-08	[inv-dar.com]	ransomhub	Link
2024-08-08	[icarasia.com]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-08	[rationalenterprise.com]	ransomhub	Link
2024-08-02	[modernceramics.com]	ransomhub	Link
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-08	[tibaitservices.com]	cactus	Link
2024-08-08	[mihlfeld.com]	cactus	Link
2024-08-08	[Horizon View Medical Center]	everest	Link
2024-08-08	[comoferta.com]	darkvault	Link
2024-08-08	[NIDEC CORPORATION]	everest	Link
2024-08-08	[mercadomineiro.com.br]	darkvault	Link
2024-08-07	[hudsoncivil.com.au]	ransomhub	Link
2024-08-07	[www.jgsummit.com.ph]	ransomhub	Link
2024-08-07	[Bayhealth Hospital]	rhysida	Link
2024-08-07	[amplicon.com]	ransomhub	Link
2024-08-06	[infotexim.pe]	ransomhub	Link
2024-08-07	[suandco.com]	madliberator	Link
2024-08-07	[Anderson Oil & Gas]	hunters	Link
2024-08-07	[bonatra.com]	killsec	Link
2024-08-07	[FatBoy Cellular]	meow	Link
2024-08-07	[KLA]	meow	Link
2024-08-07	[HUD User]	meow	Link
2024-08-06	[msprocuradores.es]	madliberator	Link
2024-08-06	[www.carri.com]	alphalocker	Link
2024-08-06	[www.consorzioinnova.it]	alphalocker	Link
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-06	[biw-burger.de]	alphalocker	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-06	[www.sobha.com]	ransomhub	Link
2024-08-06	[Alternate Energy]	play	Link
2024-08-06	[True Blue Environmental]	play	Link
2024-08-06	[Granit Design]	play	Link
2024-08-06	[KinetX]	play	Link
2024-08-06	[Omni Family Health]	hunters	Link
2024-08-06	[IOI Corporation Berhad]	fog	Link
2024-08-06	[Ziba Design]	fog	Link
2024-08-06	[Casco Antiguo]	hunters	Link
2024-08-06	[Fractalia Group]	hunters	Link
2024-08-06	[Banx Systems]	meow	Link
2024-08-05	[Silipos]	cicada3301	Link
2024-08-04	[kierlcpa.com]	lockbit3	Link
2024-08-05	[Square One Coating Systems]	cicada3301	Link
2024-08-05	[Hi-P International]	fog	Link
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	Link
2024-08-05	[HP Distribution]	incransom	Link
2024-08-05	[exco-solutions.com]	cactus	Link
2024-08-05	[Maryville Academy]	rhysida	Link
2024-08-04	[notariusze.waw.pl]	killsec	Link
2024-08-04	[Ranney School]	rhysida	Link
2024-08-03	[nursing.com]	ransomexx	Link
2024-08-03	[Bettis Asphalt]	blacksuit	Link
2024-08-03	[fcl.crs]	lockbit3	Link
2024-08-03	[CPA Tax Solutions]	meow	Link
2024-08-03	[LRN]	hunters	Link
2024-08-03	[aikenhousing.org]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-02	[David E Shambach Architect]	dragonforce	Link
2024-08-02	[Hayes Beer Distributing]	dragonforce	Link
2024-08-02	[Jangho Group]	hunters	Link
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	Link
2024-08-02	[retaildatallc.com]	ransomhub	Link
2024-08-02	[WPG Holdings]	meow	Link
2024-08-02	[National Beverage]	meow	Link
2024-08-02	[PeoplesHR]	meow	Link
2024-08-02	[Dometic Group]	meow	Link
2024-08-02	[Remitano]	meow	Link
2024-08-02	[Premier Equities]	meow	Link
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link
2024-08-02	[q-cells.de]	abyss	Link
2024-08-02	[coinbv.nl]	madliberator	Link
2024-08-01	[Valley Bulk]	cicada3301	Link
2024-08-01	[ENEA Italy]	hunters	Link
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	Link
2024-08-01	[effinghamschools.com]	ransomhub	Link
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	Link
2024-08-01	[Adorna & Guzman Dentistry]	monti	Link
2024-08-01	[Camp Susque]	medusa	Link
2024-08-01	[Ali Gohar]	medusa	Link
2024-08-01	[acsi.org]	blacksuit	Link
2024-08-01	[County Linen UK]	dispossessor	Link
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	Link
2024-08-01	[Peñoles]	akira	Link
2024-08-01	[dahlvalve.com]	cactus	Link

8 Quellen

8.1 Quellenverzeichnis

1) Cyberwatch - https://github.com/Casualtek/Cyberwatch
2) Ransomware.live - https://data.ransomware.live
3) Heise Security Alerts! - https://www.heise.de/security/alerts/
4) First EPSS - https://www.first.org/epss/
5) BSI WID - https://wid.cert-bund.de/
6) Tenable Plugins - https://www.tenable.com/plugins/
7) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

9 Impressum

Herausgeber:
Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail
info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.