Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240826

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

Notfall-Update: Microsoft behebt riskante Sicherheitslücke in Edge

Google hat die Lücke im jüngsten Chrome-Update gepatcht, es gibt Hinweise auf aktive Exploits. Daher zieht Redmond nun nach.

- Link

—

Update verfügbar: IT-Sicherheitslösung IBM QRadar SIEM ist verwundbar

IBM hat mehrere Sicherheitslücken in verschiedenen Komponenten von QRadar SIEM geschlossen.

- Link

—

Bamboo, Confluence, Jira und Co.: Atlassian schließt hochriskante Lücken

Atlassian hat Updates für zahlreiche Produkte veröffentlicht. Sie schließen als hohes Risiko geltende Sicherheitslücken etwa in Bambo, Confluence und Jira.

- Link

—

Sicherheitsupdate: Attacken auf Sonicwall-Firewalls können Crash auslösen

Um Netzwerke von Unternehmen zu schützen, sollten Admins ihre Firewalls von Sonicwall zeitnah auf den aktuellen Stand bringen.

- Link

—

Hartkodierte Zugangsdaten gefährden Solarwinds Web Help Desk

Angreifer können unbefugt auf die Kundensupport-Software Web Help Desk von Solarwinds zugreifen und Daten manipulieren.

- Link

—

5 Millionen Wordpress-Seiten gefährdet: Kritisches Leck in LiteSpeed Cache

Das Wordpress-Plug-in LiteSpeed Cache ist auf 5 Millionen Seiten installiert. Nun haben IT-Forscher eine kritische Sicherheitslücke darin entdeckt.

- Link

—

Admin-Attacken auf GitHub Enterprise Server möglich

Unter bestimmten Voraussetzungen können Angreifer Admin-Accounts von GitHub Enterprise Server kapern.

- Link

—

Angreifer können Ciscos VoIP-System Unified Communications Manager lahmlegen
Aufgrund von Sicherheitslücken sind Attacken auf mehrere Cisco-Produkte möglich. Updates sind verfügbar.
- Link

—

Google Chrome: Update stopft angegriffene Sicherheitslücke und 37 weitere
Google hat ein Update für den Webbrowser Chrome veröffentlicht. Es schließt 38 Sicherheitslücken, von denen eine bereits missbraucht wird.
- Link

—

WordPress-Plug-in: Kritische Lücke mit Höchstwertung in GiveWP geschlossen
Über eine Schwachstelle im Spenden-Plug-in GiveWP können Angreifer die Kontrolle über WordPress-Websites erlangen. Ein Sicherheitspatch ist verfügbar.
- 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	0.990030000	Link
CVE-2023-6553	0.927320000	0.990710000	Link
CVE-2023-6019	0.918710000	0.989800000	Link
CVE-2023-5360	0.902780000	0.988790000	Link
CVE-2023-52251	0.946410000	0.992890000	Link
CVE-2023-4966	0.971280000	0.998330000	Link
CVE-2023-49103	0.964030000	0.996070000	Link
CVE-2023-48795	0.965330000	0.996450000	Link
CVE-2023-47246	0.959760000	0.995180000	Link
CVE-2023-46805	0.934240000	0.991470000	Link
CVE-2023-46747	0.972900000	0.998910000	Link
CVE-2023-46604	0.964990000	0.996310000	Link
CVE-2023-4542	0.936770000	0.991680000	Link
CVE-2023-43208	0.972610000	0.998770000	Link
CVE-2023-43177	0.961750000	0.995570000	Link
CVE-2023-42793	0.970220000	0.997900000	Link
CVE-2023-41265	0.911110000	0.989320000	Link
CVE-2023-39143	0.940480000	0.992100000	Link
CVE-2023-38646	0.906950000	0.989040000	Link
CVE-2023-38205	0.953670000	0.994140000	Link
CVE-2023-38203	0.966410000	0.996740000	Link
CVE-2023-38146	0.920720000	0.989980000	Link
CVE-2023-38035	0.974920000	0.999810000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996860000	Link
CVE-2023-3519	0.965910000	0.996590000	Link
CVE-2023-35082	0.967460000	0.997050000	Link
CVE-2023-35078	0.970440000	0.997970000	Link
CVE-2023-34993	0.973130000	0.999020000	Link
CVE-2023-34960	0.928290000	0.990810000	Link
CVE-2023-34634	0.925130000	0.990500000	Link
CVE-2023-34362	0.970450000	0.997980000	Link
CVE-2023-34039	0.952470000	0.993930000	Link
CVE-2023-3368	0.937150000	0.991720000	Link
CVE-2023-33246	0.972040000	0.998520000	Link
CVE-2023-32315	0.970220000	0.997900000	Link
CVE-2023-30625	0.953610000	0.994130000	Link
CVE-2023-30013	0.965950000	0.996600000	Link
CVE-2023-29300	0.969240000	0.997550000	Link
CVE-2023-29298	0.941540000	0.992240000	Link
CVE-2023-28432	0.911820000	0.989370000	Link
CVE-2023-28343	0.933130000	0.991360000	Link
CVE-2023-28121	0.909500000	0.989180000	Link
CVE-2023-27524	0.970600000	0.998040000	Link
CVE-2023-27372	0.973470000	0.999140000	Link
CVE-2023-27350	0.969720000	0.997730000	Link
CVE-2023-26469	0.951470000	0.993710000	Link
CVE-2023-26360	0.963510000	0.995930000	Link
CVE-2023-26035	0.969020000	0.997460000	Link
CVE-2023-25717	0.954250000	0.994240000	Link
CVE-2023-25194	0.967920000	0.997180000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996040000	Link
CVE-2023-24489	0.973820000	0.999290000	Link
CVE-2023-23752	0.956380000	0.994630000	Link
CVE-2023-23333	0.962300000	0.995660000	Link
CVE-2023-22527	0.968780000	0.997410000	Link
CVE-2023-22518	0.965970000	0.996610000	Link
CVE-2023-22515	0.972340000	0.998650000	Link
CVE-2023-21839	0.955020000	0.994390000	Link
CVE-2023-21554	0.955880000	0.994550000	Link
CVE-2023-20887	0.970670000	0.998050000	Link
CVE-2023-1671	0.964660000	0.996200000	Link
CVE-2023-0669	0.969760000	0.997740000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 23 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

—

Fri, 23 Aug 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um falsche Informationen darzustellen und beliebigen Code auszuführen.

- Link

—

Fri, 23 Aug 2024

[NEU] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift

Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 23 Aug 2024

[UPDATE] [hoch] ImageMagick: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Fri, 23 Aug 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Fri, 23 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

—

Fri, 23 Aug 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 23 Aug 2024

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 23 Aug 2024

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

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

- Link

—

Fri, 23 Aug 2024

[NEU] [hoch] SonicWall SonicOS: Schwachstelle ermöglicht Offenlegung von Informationen und Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SonicWall SonicOS ausnutzen, um Informationen offenzulegen und um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 22 Aug 2024

[NEU] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, Daten zu manipulieren, vertrauliche Informationen offenzulegen, eine Man-in-the-Middle-Situation zu schaffen, Sicherheits-maßnahmen zu umgehen oder eine Denial-of-Service-Situation zu schaffen.

- Link

—

Thu, 22 Aug 2024

[NEU] [hoch] Cisco Unified Communications Manager (CUCM): Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Cisco Unified Communications Manager (CUCM) ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Thu, 22 Aug 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, UI-Spoofing zu betreiben, Sicherheitsmechanismen zu umgehen und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Thu, 22 Aug 2024

[UPDATE] [hoch] Microsoft Exchange Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Exchange Server 2013, Microsoft Exchange Server 2016 und Microsoft Exchange Server 2019 ausnutzen, um beliebigen Programmcode auszuführen, um seine Privilegien zu erhöhen und um Informationen offenzulegen.
- Link

—

Thu, 22 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.
- Link

—

Thu, 22 Aug 2024

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.
- Link

—

Thu, 22 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

—

Thu, 22 Aug 2024

[NEU] [UNGEPATCHT] [kritisch] FRRouting Project FRRouting: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Zustand zu erzeugen und potenziell beliebigen Programmcode auszuführen.
- Link

—

Thu, 22 Aug 2024

[NEU] [UNGEPATCHT] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 21 Aug 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/25/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2024:3003-1)]	critical
8/24/2024	[Fedora 40 : zabbix (2024-8382d1b267)]	critical
8/24/2024	[Fedora 39 : zabbix (2024-c89d2ecdea)]	critical
8/23/2024	[WordPress Plugin ‘LiteSpeed Cache’ < 6.4 Privilege Escalation]	critical
8/23/2024	[Ivanti Avalanche < 6.4.4 Multiple Vulnerabilities]	critical
8/23/2024	[Acronis Cyber Infrastructure 5.1.x < 5.1.1-71 / 5.2.x < 5.2.1-69 / 5.3.x < 5.3.1-53 / 5.4.x < 5.4.4-132 / < 5.0.1-61 (SEC-6452)]	critical
8/25/2024	[SUSE SLED12 / SLES12 Security Update : libofx (SUSE-SU-2024:3007-1)]	high
8/25/2024	[SUSE SLES12 Security Update : fetchmail (SUSE-SU-2024:3006-1)]	high
8/25/2024	[SUSE SLES12 Security Update : expat (SUSE-SU-2024:3004-1)]	high
8/25/2024	[SUSE SLES15 Security Update : xen (SUSE-SU-2024:3001-1)]	high

Datum	Schwachstelle	Bewertung
8/25/2024	[openSUSE 15 Security Update : chromium, gn, rust-bindgen (openSUSE-SU-2024:0254-2)]	high
8/25/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0258-2)]	high
8/24/2024	[Photon OS 4.0: Libtiff PHSA-2024-4.0-0673]	high
8/24/2024	[Photon OS 3.0: Libtiff PHSA-2024-3.0-0784]	high
8/24/2024	[Photon OS 5.0: Libtiff PHSA-2024-5.0-0354]	high
8/24/2024	[Photon OS 4.0: Linux PHSA-2024-4.0-0669]	high
8/23/2024	[Cisco Unified Communications Manager DoS (cisco-sa-cucm-dos-kkHq43We)]	high
8/23/2024	[Autodesk AutoCAD 25.0.x < 25.0.101.0 (2025.1) (adsk-sa-2024-0014)]	high
8/23/2024	[Autodesk DWG TrueView 25.0.x < 25.0.101.0 (2025.1) (adsk-sa-2024-0014)]	high
8/23/2024	[Siemens JT2Go < 2312.0005 Multiple Vulnerabilities (SSA-856475)]	high
8/23/2024	[Debian dsa-5757 : chromium - security update]	high
8/23/2024	[F5 Networks BIG-IP : Apache HTTPD vulnerability (K000140784)]	high
8/23/2024	[Ubuntu 20.04 LTS : Linux kernel (Oracle) vulnerabilities (USN-6974-2)]	high
8/23/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6972-3)]	high
8/23/2024	[Ubuntu 18.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6973-2)]	high
8/23/2024	[Microsoft Edge (Chromium) < 128.0.2739.42 Multiple Vulnerabilities]	high
8/23/2024	[Siemens (CVE-2024-41977)]	high
8/23/2024	[Siemens (CVE-2024-41976)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 23 Aug 2024

Ray cpu_profile Command Injection

This Metasploit module demonstrates a command injection vulnerability in Ray via cpu_profile.

- Link

—

” “Fri, 23 Aug 2024

Ray Agent Job Remote Code Execution

This Metasploit modules demonstrates remote code execution in Ray via the agent job submission endpoint. This is intended functionality as Ray’s main purpose is executing arbitrary workloads. By default Ray has no authentication.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Information Disclosure

DiCal-RED version 4009 provides a network server on TCP port 2101. This service does not seem to process any input, but it regularly sends data to connected clients. This includes operation messages when they are processed by the device. An unauthenticated attacker can therefore gain information about current emergency situations and possibly also emergency vehicle positions or routes.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Log Disclosure

DiCal-RED version 4009 is vulnerable to unauthorized log access and other files on the device’s file system due to improper authentication checks.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Path Traversal

DiCal-RED version 4009 has an administrative web interface that is vulnerable to path traversal attacks in several places. The functions to download or display log files can be used to access arbitrary files on the device’s file system. The upload function for new license files can be used to write files anywhere on the device’s file system - possibly overwriting important system configuration files, binaries or scripts. Replacing files that are executed during system operation results in a full compromise of the whole device.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Cryptography Failure

DiCal-RED version 4009 provides an administrative web interface that requests the administrative system password before it can be used. Instead of submitting the user-supplied password, its MD5 hash is calculated on the client side and submitted. An attacker who knows the hash of the correct password but not the password itself can simply replace the value of the password URL parameter with the correct hash and subsequently gain full access to the administrative web interface.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Weak Hashing

DiCal-RED version 4009 has a password that is stored in the file /etc/deviceconfig as a plain MD5 hash, i.e. without any salt or computational cost function.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Missing Authentication

DiCal-RED version 4009 provides an FTP service on TCP port 21. This service allows anonymous access, i.e. logging in as the user ”anonymous” with an arbitrary password. Anonymous users get read access to the whole file system of the device, including files that contain sensitive configuration information, such as /etc/deviceconfig. The respective process on the system runs as the system user ”ftp”. Therefore, a few files with restrictive permissions are not accessible via FTP.

- Link

—

” “Fri, 23 Aug 2024

DiCal-RED 4009 Missing Authentication

DiCal-RED version 4009 provides a Telnet service on TCP port 23. This service grants access to an interactive shell as the system’s root user and does not require authentication.

- Link

—

” “Fri, 23 Aug 2024

PlantUML 1.2024.6 Cross Site Scripting

PlantUML version 1.2024.6 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 23 Aug 2024

Crime Complaints Reporting Management System 1.0 Shell Upload

Crime Complaints Reporting Management System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 23 Aug 2024

Courier Management System 1.0 Cross Site Request Forgery

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

- Link

—

” “Fri, 23 Aug 2024

Company Visitor Management 1.0 SQL Injection

Company Visitor Management version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 23 Aug 2024

CMSsite 1.0 Shell Upload

CMSsite version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 23 Aug 2024

CMS RIMI 1.3 Cross Site Request Forgery / File Upload

CMS RIMI version 1.3 suffers from cross site request forgery and arbitrary file upload vulnerabilities.

- Link

—

” “Fri, 23 Aug 2024

Client Management System 1.0 SQL Injection

Client Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 23 Aug 2024

CCMS Project 1.0 SQL Injection

CCMS Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 23 Aug 2024

Biobook Social Networking Site 1.0 SQL Injection

Biobook Social Networking Site version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 22 Aug 2024

DIAEnergie 1.10 SQL Injection

This Metasploit module exploit a remote SQL injection vulnerability in the CBEC service of DIAEnergie versions 1.10 and below from Delta Electronics. The commands will get executed in the context of NT AUTHORITY\SYSTEM.

- Link

—

” “Thu, 22 Aug 2024

SPIP 4.2.12 Remote Code Execution

This Metasploit module exploits a remote code execution vulnerability in SPIP versions up to and including 4.2.12. The vulnerability occurs in SPIP’s templating system where it incorrectly handles user-supplied input, allowing an attacker to inject and execute arbitrary PHP code. This can be achieved by crafting a payload manipulating the templating data processed by the echappe_retour() function, invoking traitements_previsu_php_modeles_eval(), which contains an eval() call.

- Link

—

” “Thu, 22 Aug 2024

AVMS Project 1.0 SQL Injection

AVMS Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 22 Aug 2024

Online Survey System 1.0 Cross Site Request Forgery

Online Survey System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 22 Aug 2024

Online Shopping System Master 1.0 Cross Site Request Forgery

Online Shopping System Master version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 22 Aug 2024

Online Banking System 1.0 Arbitrary File Upload

Online Banking System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Thu, 22 Aug 2024

Online ID Generator 1.0 Cross Site Request Forgery

Online ID Generator version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 23 Aug 2024

ZDI-24-1181: Axis Communications Autodesk Plugin Exposure of Sensitive Information Authentication Bypass Vulnerability

- Link

—

” “Fri, 23 Aug 2024

ZDI-24-1180: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Fri, 23 Aug 2024

ZDI-24-1179: Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 23 Aug 2024

ZDI-24-1178: Qualcomm Wi-Fi SON LDB Service Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 23 Aug 2024

ZDI-24-1177: Amazon AWS CloudFormation Templates Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Fri, 23 Aug 2024

ZDI-24-1176: Amazon AWS aws-glue-with-s2s-vpn Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1175: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1174: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1173: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1172: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1171: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1170: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1169: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote

Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1168: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1167: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1166: Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1165: Allegra getLinkText Server-Side Template Injection Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1164: Allegra unzipFile Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1163: Allegra loadFieldMatch Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1162: Allegra renderFieldMatch Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1161: Linux Kernel vmwgfx Driver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1160: Apple WebKit WebCodecs VideoFrame Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1159: G DATA Total Security Scan Server Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1158: Rockwell Automation ThinManager ThinServer Unrestricted File Upload Remote Code Execution Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1157: Rockwell Automation ThinManager ThinServer Arbitrary File Creation Privilege Escalation Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1156: Rockwell Automation ThinManager ThinServer Arbitrary File Read Information Disclosure Vulnerability

- Link

—

” “Thu, 22 Aug 2024

ZDI-24-1155: PaperCut NG image-handler Directory Traversal Local Privilege Escalation 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
2024-08-21	Groupe Cirano	[REU]	Link
2024-08-21	Halliburton	[USA]	Link
2024-08-19	BVI Electricity Corporation (BVIEC)	[VGB]	Link
2024-08-18	Lagoon	[NCL]	Link
2024-08-18	Ponta Grossa	[BRA]	Link
2024-08-18	Pittsburg	[USA]	Link
2024-08-17	Bella Vista	[USA]	Link
2024-08-17	Microchip Technology Incorporated	[USA]	Link
2024-08-17	Octave	[FRA]	Link
2024-08-16	Contarina	[ITA]	Link
2024-08-16	Shoshone-Bannock Tribes	[USA]	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
2024-08-11	Itu	[BRA]	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

Datum	Opfer	Land	Information
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
2024-08-04	Regent Caravans	[AUS]	Link
2024-08-03	Xtrim	[ECU]	Link
2024-08-02	Ihecs	[BEL]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-26	[onedayonly.co.za]	killsec	Link
2024-08-26	[Affordable Tools]	rhysida	Link
2024-08-25	[prasarana.com.my]	ransomhub	Link
2024-08-19	[Penn Veterinary Supply INC]	qilin	Link
2024-08-21	[Meli (BCYF & Bethany)]	qilin	Link
2024-08-25	[dt-technologies]	qilin	Link
2024-08-26	[autonomous.ai]	killsec	Link
2024-08-25	[Sable International]	bianlian	Link
2024-08-18	[The University and College Union]	incransom	Link
2024-08-25	[EPS Tech R&D]	handala	Link
2024-08-24	[nwcsb.com]	blacksuit	Link
2024-08-23	[Myelec Electrical]	lynx	Link
2024-08-24	[www.curvc.com]	ElDorado	Link
2024-08-24	[Eagle Safety Eyewear]	ElDorado	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-18	[Wallace Construction Specialties (wcs.local))]	lynx	Link
2024-08-18	[Bay Sales (cog.local)]	lynx	Link
2024-08-18	[PBS group]	lynx	Link
2024-08-18	[Health Quality Council]	incransom	Link
2024-08-24	[HBGJEWISHCOMMUN]	helldown	Link
2024-08-24	[ingotbrokers.com]	darkvault	Link
2024-08-24	[Hofmann Malerei AG]	cicada3301	Link
2024-08-24	[Studio Legale Associato Isolabella]	bianlian	Link
2024-08-22	[HL Lawson & Sons]	incransom	Link
2024-08-23	[terralogs.com.br]	killsec	Link
2024-08-23	[Chama Gaucha]	cicada3301	Link
2024-08-23	[idahopacific.com]	abyss	Link
2024-08-23	[barryavenueplating]	helldown	Link
2024-08-23	[rsk-immobilien]	helldown	Link
2024-08-23	[Crimson Interactive]	hunters	Link
2024-08-23	[www.seaeng.com]	dAn0n	Link
2024-08-23	[Stjamesplace.org]	cloak	Link
2024-08-23	[Saeilo]	metaencryptor	Link
2024-08-22	[schoolrush.com]	killsec	Link
2024-08-22	[Life University]	metaencryptor	Link
2024-08-22	[Sherwood Stainless & Aluminium]	dragonforce	Link
2024-08-22	[Igloo Cellulose]	dragonforce	Link
2024-08-22	[Raifalsa-Alelor]	dragonforce	Link
2024-08-22	[Deane Roofing and Cladding]	dragonforce	Link
2024-08-22	[instadriver.co]	killsec	Link
2024-08-22	[cincinnatipainphysicians]	helldown	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-22	[Don’t Waste Group]	incransom	Link
2024-08-22	[Kronick Moskovitz Tiedemann & Girard]	rhysida	Link
2024-08-22	[UFCW Local 135]	cicada3301	Link
2024-08-22	[EBA Ernest Bland Associates]	cicada3301	Link
2024-08-22	[level.game]	killsec	Link
2024-08-22	[antaeustravel.com]	blackout	Link
2024-08-22	[rylandpeters.com]	apt73	Link
2024-08-22	[saudi arabia(general secretariat of the military service council)]	ransomhub	Link
2024-08-22	[Engedi]	rhysida	Link
2024-08-22	[EPS Tech confidential source code (military)]	handala	Link
2024-08-16	[policiaauxiliarcusaem.com.mx]	lockbit3	Link
2024-08-14	[Larc]	incransom	Link
2024-08-22	[kbosecurity.co.uk]	helldown	Link
2024-08-22	[khonaysser.com]	helldown	Link
2024-08-21	[beinlaw.co.il - Prof. Bein & Co.]	BrainCipher	Link
2024-08-21	[The SMS Group]	play	Link
2024-08-21	[Grid Subject Matter Experts]	play	Link
2024-08-21	[Quilvest Capital Partners]	play	Link
2024-08-21	[Armour Coatings]	play	Link
2024-08-21	[RCG]	play	Link
2024-08-21	[Policy Administration Solutions]	play	Link
2024-08-21	[Dunlop Aircraft Tyres]	cloak	Link
2024-08-21	[Vibo.dk]	cloak	Link
2024-08-21	[Hvb-ingenieure.de]	cloak	Link
2024-08-21	[Westermans.com]	cloak	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-21	[Jinny Corporation]	akira	Link
2024-08-21	[BARRYAVEPLATING]	helldown	Link
2024-08-21	[RSK-IMMOBILIEN]	helldown	Link
2024-08-20	[capitalfund1.com]	ransomhub	Link
2024-08-21	[www.pindrophearing.co.uk]	apt73	Link
2024-08-21	[www.banhampoultry.co.uk]	ransomhub	Link
2024-08-21	[kidkraft.com]	lynx	Link
2024-08-21	[Luigi Convertini]	ciphbit	Link
2024-08-21	[Findel]	cicada3301	Link
2024-08-21	[HOERBIGER Holding]	akira	Link
2024-08-21	[Olympus Financial]	rhysida	Link
2024-08-21	[spvmhc.org]	abyss	Link
2024-08-21	[Burns Industrial Equipment]	meow	Link
2024-08-21	[globacap.com]	apt73	Link
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	[ATP]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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]	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-08-14	[mmtransport.com]	dAn0n	Link
2024-08-14	[Riley Pope & Laney]	cicada3301	Link
2024-08-13	[hugwi]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-13	[Erie Meats]	play	Link
2024-08-13	[M??? ????k ??????]	play	Link
2024-08-13	[SCHLATTNER]	helldown	Link
2024-08-13	[deganis]	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
2024-08-09	[cbmm]	helldown	Link
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	Link
2024-08-11	[briju]	helldown	Link
2024-08-11	[vindix]	helldown	Link
2024-08-11	[Albatros]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.