Cybersecurity Morgenreport

Ausgabe: 20230927

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

Security-News

Heise - Security-Alert

Softwareentwicklung: Angreifer können über TeamCity-Lücke Sourcecode stehlen
In einer aktuellen Version von TeamCity haben die Verantwortlichen ein gefährliches Sicherheitsproblem gelöst.
- Link

—

Sicherheitslücke: Datenleaks auf Drupal-Websites möglich
Unter bestimmten Voraussetzungen können Angreifer mit dem Content Management System Drupal erstellte Seiten attackieren. Abgesicherte Versionen sind verfügbar.
- Link

—

Qnap warnt vor Codeschmuggel durch Schwachstellen
Qnap warnt vor Sicherheitslücken im QTS-Betriebssystem und der Multimedia Console, durch die Angreifer Schadcode einschleusen können.
- Link

—

Sicherheitsupdate: Authentifizierung von HPE OneView umgehbar
Die IT-Infrastrukturmanagementlösung OneView von HPE ist verwundbar. Der Entwickler hat zwei kritische Sicherheitslücken geschlossen.
- Link

—

Sicherheitsupdate: Passwort-Lücke bedroht Nagios XI
Angreifer können die Server-Monitoring-Lösung Nagios XI attackieren. Eine dagegen abgesicherte Version ist verfügbar.
- Link

—

MOVEit Transfer: Schwachstellen ermöglichen Angreifern Datenschmuggel
Neue MOVEit Transfer-Versionen schließen teils hochriskante Sicherheitslücken. IT-Verantwortliche sollten sie zügig installieren.
- Link

—

Atlassian stopft Sicherheitslecks in Bitbucket, Confluence und Jira
Atlassian warnt vor Sicherheitslücken in Bitbucket, Confluence und Jira. Aktualisierte Fassungen dichten sie ab.
- Link

—

Gitlab warnt vor kritischer Sicherheitslücke
Eine kritische Sicherheitslücke bedroht die Enterprise-Anwender des Repository-Diensts Gitlab. Kunden sollten unverzüglich ein Update einspielen.
- Link

—

Jetzt patchen! Angreifer attackieren Trend Micro Apex One & Co.
Eine kritische Sicherheitslücke bedroht verschiedene AV-Produkte von Trend Micro. Sicherheitsupdates stehen zum Download bereit.
- Link

—

Jetzt patchen! Tausende Juniper-Firewalls immer noch ohne Sicherheitsupdate
Aufgrund eines neuen Exploits sind Attacken auf Juniper-Firewalls jetzt noch einfacher. Sicherheitspatches sind verfügbar.
- Link

—

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-38035	0.970110000	0.996480000	Link
CVE-2023-35078	0.955330000	0.991610000	Link
CVE-2023-34362	0.920100000	0.985870000	Link
CVE-2023-33246	0.971460000	0.997160000	Link
CVE-2023-32315	0.960810000	0.992960000	Link
CVE-2023-28771	0.926550000	0.986690000	Link
CVE-2023-27524	0.936870000	0.988100000	Link
CVE-2023-27372	0.971740000	0.997340000	Link
CVE-2023-27350	0.970860000	0.996850000	Link
CVE-2023-26469	0.918080000	0.985700000	Link
CVE-2023-26360	0.900410000	0.984070000	Link
CVE-2023-25717	0.958870000	0.992440000	Link
CVE-2023-25194	0.924830000	0.986440000	Link
CVE-2023-24489	0.967770000	0.995440000	Link
CVE-2023-21839	0.946810000	0.989670000	Link
CVE-2023-21823	0.907830000	0.984700000	Link
CVE-2023-21554	0.961360000	0.993090000	Link
CVE-2023-20887	0.944590000	0.989290000	Link
CVE-2023-0669	0.967330000	0.995280000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 26 Sep 2023
[UPDATE] [hoch] Node.js: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Tue, 26 Sep 2023
[UPDATE] [hoch] binutils: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder sonstige Auswirkungen zu verursachen.
- Link

—

Tue, 26 Sep 2023
[NEU] [hoch] docker: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in docker ausnutzen, um beliebigen Programmcode auszuführen und Privilegien zu erhöhen.
- Link
—
Tue, 26 Sep 2023
[NEU] [hoch] docker: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [kritisch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und seine Privilegien zu erweitern.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen, Sicherheitsmechanismen zu umgehen, seine Privilegien zu erweitern und um beliebigen Code auszuführen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [kritisch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und seine Privilegien zu erweitern
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft Azure DevOps Server, Microsoft NuGet, Microsoft Visual Studio und Microsoft Visual Studio Code ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, seine Rechte zu erweitern und Daten zu manipulieren.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Rechte zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Daten zu Manipulieren und einen Denial-of-Service-Zustand zu verursachen.
- Link
—
Tue, 26 Sep 2023
[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, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Tue, 26 Sep 2023

[UPDATE] [hoch] Microsoft Windows: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Dateien zu manipulieren oder beliebigen Code auszuführen.
- Link
—
Tue, 26 Sep 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung, Dos oder Speicheränderung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.
- Link
—
Mon, 25 Sep 2023
[NEU] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 25 Sep 2023
[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.
- Link
—
Mon, 25 Sep 2023
[UPDATE] [hoch] Apache HttpComponents: Schwachstelle ermöglicht Täuschung des Nutzers
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache HttpComponents ausnutzen, um den Nutzer zu täuschen.
- Link
—
Mon, 25 Sep 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Mon, 25 Sep 2023
[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/26/2023	[Siemens InsydeH2O Privilege Escalation (CVE-2020-5955)]	critical
9/26/2023	[Siemens InsydeH2O SMM Privilege Escalation (CVE-2021-43323)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2023-22613)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2023-22614)]	high
9/26/2023	[Siemens InsydeH2O SMM Privilege Escalation (CVE-2022-24069)]	high
9/26/2023	[Siemens InsydeH2O Cleartext Storage of Sensitive Information (CVE-2023-31041)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2023-22615)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32470)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32469)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32953)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-45971)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-43522)]	high
9/26/2023	[Siemens InsydeH2O Arbitrary Code Execution (CVE-2022-36338)]	high
9/26/2023	[Siemens InsydeH2O Arbitrary Code Execution (CVE-2022-35408)]	high
9/26/2023	[Siemens InsydeH2O Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-33625)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-45970)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2022-35895)]	high
9/26/2023	[Siemens InsydeH2O SMM Privilege Escalation (CVE-2021-42060)]	high
9/26/2023	[Siemens InsydeH2O SMM Privilege Escalation (CVE-2021-42113)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-42554)]	high
9/26/2023	[Siemens InsydeH2O Allocation of Resources Without Limits or Throttling (CVE-2021-41840)]	high
9/26/2023	[Siemens InsydeH2O Inclusion of Functionality from Untrusted Control Sphere (CVE-2021-33626)]	high
9/26/2023	[Siemens InsydeH2O Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-41838)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2022-24030)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2023-22612)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32476)]	high
9/26/2023	[Siemens InsydeH2O Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-41839)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2022-24031)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32954)]	high
9/26/2023	[Siemens InsydeH2O Inclusion of Functionality from Untrusted Control Sphere (CVE-2021-41841)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32471)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32478)]	high
9/26/2023	[Siemens InsydeH2O Improper Input Validation (CVE-2020-5956)]	high
9/26/2023	[Siemens InsydeH2O Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-41837)]	high
9/26/2023	[Siemens InsydeH2O Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-33627)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32474)]	high

Datum	Schwachstelle	Bewertung
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32477)]	high
9/26/2023	[Siemens InsydeH2O Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2022-32955)]	high
9/26/2023	[Siemens InsydeH2O SMM Privilege Escalation (CVE-2020-5953)]	high
9/26/2023	[Siemens InsydeH2O Insufficient Input Validation (CVE-2023-22616)]	high
9/26/2023	[Siemens InsydeH2O Improper Input Validation (CVE-2022-36448)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-45969)]	high
9/26/2023	[Siemens InsydeH2O Out-of-bounds Write (CVE-2021-43615)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Mon, 25 Sep 2023
RoyalTSX 6.0.1 RTSZ File Handling Heap Memory Corruption
RoyalTSX version 6.0.1 suffers from an RTSZ file handling heap memory corruption vulnerability. The application receives SIGABRT after the RAPortCheck.createNWConnection() function is handling the SecureGatewayHost object in the RoyalTSXNativeUI. When the hostname has an array of around 1600 bytes and the Test Connection is clicked the application crashes instantly.
- Link
—
” “Mon, 25 Sep 2023
OPNsense 23.1.11_1 / 23.7.3 / 23.7.4 Cross Site Scripting / Privilege Escalation
OPNsense versions 23.1.11_1, 23.7.3, and 23.7.4 suffer from cross site scripting vulnerabilities that can allow for privilege escalation.
- Link
—
” “Mon, 25 Sep 2023
LogoBee CMS 0.2 Cross Site Scripting
LogoBee CMS version 0.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 25 Sep 2023
Lamano LMS 0.1 Insecure Settings
Lamano LMS version 0.1 suffers from an ignored default credential vulnerability.
- Link
—
” “Fri, 22 Sep 2023
Elasticsearch 8.5.3 Stack Overflow
Elasticsearch version 8.5.3 stack overflow proof of concept exploit.
- Link
—
” “Fri, 22 Sep 2023
Taskhub 2.8.8 Cross Site Scripting
Taskhub version 2.8.8 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 21 Sep 2023
TOTOLINK Wireless Routers Remote Command Execution
Multiple TOTOLINK network products contain a command injection vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the command parameter. After exploitation, an attacker will have full access with the same user privileges under which the webserver is running - which is typically root.
- Link
—
” “Thu, 21 Sep 2023
Luxcal Event Calendar 3.2.3 Cross Site Request Forgery
Luxcal Event Calendar version 3.2.3 suffers from a cross site request forgery vulnerability.
- Link
—
” “Wed, 20 Sep 2023
Lamano CMS 2.0 Cross Site Request Forgery
Lamano CMS version 2.0 suffers from a cross site request forgery vulnerability.
- Link
—
” “Wed, 20 Sep 2023
WordPress Theme My Login 2FA Brute Force
WordPress Theme My Login 2FA plugin versions prior to 1.2 suffer from a brute forcing vulnerability.
- Link
—

” “Tue, 19 Sep 2023

Apache Airflow 1.10.10 Remote Code Execution

This Metasploit module exploits an unauthenticated command injection vulnerability by combining two critical vulnerabilities in Apache Airflow version 1.10.10. The first, CVE-2020-11978, is an authenticated command injection vulnerability found in one of Airflow's example DAGs, ”example_trigger_target_dag”, which allows any authenticated user to run arbitrary OS commands as the user running Airflow Worker/Scheduler. The second, CVE-2020-13927, is a default setting of Airflow 1.10.10 that allows unauthenticated access to Airflow's Experimental REST API to perform malicious actions such as creating the vulnerable DAG above. The two CVEs taken together allow vulnerable DAG creation and command injection, leading to unauthenticated remote code execution.

- Link

—

” “Tue, 19 Sep 2023

Lexmark Device Embedded Web Server Remote Code Execution

An unauthenticated remote code execution vulnerability exists in the embedded webserver in certain Lexmark devices through 2023-02-19. The vulnerability is only exposed if, when setting up the printer or device, the user selects ”Set up Later” when asked if they would like to add an Admin user. If no Admin user is created, the endpoint /cgi-bin/fax_change_faxtrace_settings is accessible without authentication. The endpoint allows the user to configure a number of different fax settings. A number of the configurable parameters on the page fail to be sanitized properly before being used in a bash eval statement, allowing for an unauthenticated user to run arbitrary commands.

- Link

—

” “Tue, 19 Sep 2023

WordPress Essential Blocks 4.2.0 / Essential Blocks Pro 1.1.0 PHP Object Injection

WordPress Essential Blocks plugin versions 4.2.0 and below and Essential Blocks Pro versions 1.1.0 and below suffer from multiple PHP object injection vulnerabilities.

- Link

—

” “Tue, 19 Sep 2023

Taskhub 2.8.7 SQL Injection

Taskhub version 2.8.7 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 19 Sep 2023

Packers And Movers Management System 1.0 SQL Injection

Packers and Movers Management System version 1.0 suffers from a remote blind SQL injection vulnerability. Proof of concept exploit written in python included.

- Link

—

” “Tue, 19 Sep 2023

Super Store Finder 3.7 Remote Command Execution

Super Store Finder versions 3.7 and below suffer from a remote command execution vulnerability.

- Link

—

” “Tue, 19 Sep 2023

Lamano CMS 2.0 SQL Injection

Lamano CMS version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 19 Sep 2023

Lacabane 1.0 SQL Injection

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

- Link

—

” “Tue, 19 Sep 2023

Free And Open Source Inventory Management System 1.0 SQL Injection

Free and Open Source Inventory Management System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—
” “Mon, 18 Sep 2023
Atos Unify OpenScape Code Execution / Missing Authentication
Atos Unify OpenScape Session Border Controller, Atos Unify OpenScape Branch, and Atos Unify OpenScape BCF suffer from remote code execution and missing authentication vulnerabilities. Atos OpenScape SBC versions before 10 R3.3.0, Branch version 10 versions before R3.3.0, and BCF version 10 versions before 10 R10.10.0 are affected.
- Link
—
” “Mon, 18 Sep 2023
PTC - Codebeamer Cross Site Scripting
PTC - Codebeamer versions 22.10-SP7 and below, 22.04-SP5 and below, and 21.09-SP13 and below suffer from a cross site scripting vulnerability.
- Link
—
” “Mon, 18 Sep 2023
Ivanti Avalanche MDM Buffer Overflow
This Metasploit module exploits a buffer overflow condition in Ivanti Avalanche MDM versions prior to 6.4.1. An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in arbitrary code execution with the NT/AUTHORITY SYSTEM permissions. This vulnerability occurs during the processing of 3/5/8/100/101/102 item data types. The program tries to copy the item data using qmemcopy to a fixed size data buffer on stack. Upon successful exploitation the attacker gains full access to the target system. This vulnerability has been tested against Ivanti Avalanche MDM version 6.4.0.0 on Windows 10.
- Link
—
” “Mon, 18 Sep 2023
Razer Synapse Race Condition / DLL Hijacking
Razer Synapse versions before 3.8.0428.042117 (20230601) suffer from multiple vulnerabilities. Due to an unsafe installation path, improper privilege management, and a time-of-check time-of-use race condition, the associated system service ”Razer Synapse Service” is vulnerable to DLL hijacking. As a result, local Windows users can abuse the Razer driver installer to obtain administrative privileges on Windows.
- Link
—
” “Mon, 18 Sep 2023
KPOT Stealer CMS 2.0 Directory Traversal
KPOT Stealer CMS 2.0 suffers from a directory traversal vulnerability.
- Link
—
” “Mon, 18 Sep 2023
KPK CMS 1.0 SQL Injection
KPK CMS version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
”

0-Day

Die Hacks der Woche

mit Martin Haunschmid

Good Guy Debugmodus deanonymisiert einen Ransomware-Programmierer | Die webp-Lücke

Zum Youtube Video

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2023-09-27	La cristallerie Baccarat	[FRA]	Link
2023-09-25	Baruch College	[USA]	Link
2023-09-24	Université Fédérale du Mato Grosso do Sul (UFMS)	[BRA]	Link
2023-09-22	Philippine Health Insurance Corporation (PhilHealth)	[PHL]	Link
2023-09-22	Le gouvernement des Bermudes	[BMU]	Link
2023-09-22	Maries County Courthouse	[USA]	Link
2023-09-22	KITV 4 Island News	[USA]	Link
2023-09-21	Ville de Morlaix	[FRA]	Link
2023-09-20	Conseil des consommateurs	[HKG]	Link
2023-09-19	Eventcombo	[USA]	Link
2023-09-19	Hochschule Furtwangen (HFU)	[DEU]	Link
2023-09-19	Air Canada	[CAN]	Link
2023-09-19	La Fondation de France	[FRA]	Link
2023-09-19	Wacoal	[JPN]	Link
2023-09-19	Duale Hochschule Baden Württemberg	[DEU]	Link
2023-09-18	La ville de Pittsburg	[USA]	Link
2023-09-18	Somagic	[FRA]	Link
2023-09-17	Grupo Xcaret	[MEX]	Link
2023-09-15	La Cour pénale internationale (CPI)	[NLD]	Link
2023-09-14	Auckland Transport	[NZL]	Link
2023-09-14	Royal HZPC Group	[NLD]	Link
2023-09-12	Un prestataire de Pelmorex Corp.	[CAN]	Link
2023-09-12	IFX Networks	[COL]	Link
2023-09-11	MGM Resorts	[USA]	Link
2023-09-11	Partenaire de moBiel	[DEU]	Link
2023-09-11	Le système d'information judiciaire régional (REJIS) du comté de St. Louis	[USA]	Link
2023-09-11	Zetema Progetto Cultura	[ITA]	Link
2023-09-11	Agence de relations publiques ikp	[AUT]	Link
2023-09-07	Le groupe hospitalier Saint-Vincent à Strasbourg	[FRA]	Link
2023-09-06	L'académie St Augustine à Maidstone	[GBR]	Link
2023-09-06	Comté de Hinds	[USA]	Link
2023-09-06	ORBCOMM	[USA]	Link
2023-09-05	Mairie de Séville	[ESP]	Link
2023-09-05	Financial Services Commission (FSC)	[JAM]	Link
2023-09-05	Decatur Independent School District (DISD)	[USA]	Link
2023-09-05	Thermae 2000	[NLD]	Link
2023-09-04	Maiden Erlegh Trust	[GBR]	Link
2023-09-01	Comitato Elettrotecnico Italiano (CEI)	[ITA]	Link
2023-09-01	Secrétariat de l'environnement et des ressources naturelles (Semarnat)	[MEX]	Link

Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-25	[Acoustic Center]	medusa	Link
2023-09-26	[LANDSTAR POWER ONTARIO INC]	medusa	Link
2023-09-21	[Scara]	noescape	Link
2023-09-26	[Robins & Morton]	dunghill_leak	Link
2023-09-26	[CannonDesign]	dunghill_leak	Link
2023-09-26	[Siamese Asset]	qilin	Link
2023-09-26	[Roper & Vertafore]	dunghill_leak	Link
2023-09-26	[Go-Ahead Group]	dunghill_leak	Link
2023-09-26	[GCserv.com]	alphv	Link
2023-09-26	[Ropertech.com & Vertafore.com]	dunghill_leak	Link
2023-09-26	[Orthum Bau]	cactus	Link
2023-09-26	[Astro Lighting]	cactus	Link
2023-09-26	[Istituto Prosperius]	rhysida	Link
2023-09-26	[Woody Anderson Ford]	alphv	Link
2023-09-26	[Nordic Security Services]	alphv	Link
2023-09-26	[Prestige Care]	alphv	Link
2023-09-26	[Kramer Tree Specialists, Inc]	bianlian	Link
2023-09-26	[Lutheran Church and Preschool]	bianlian	Link
2023-09-26	[Saint Mark Catholic Church]	bianlian	Link
2023-09-26	[BestPack Packaging]	alphv	Link
2023-09-26	[Arazoza Brothers]	losttrust	Link
2023-09-26	[Popovici Niu Stoica & Asociaii]	losttrust	Link
2023-09-26	[Procab]	losttrust	Link
2023-09-26	[Hoosier Uplands Economic Development]	losttrust	Link
2023-09-26	[Oasys Technologies]	losttrust	Link
2023-09-26	[Merced City School District]	losttrust	Link
2023-09-26	[Morgan School District]	losttrust	Link
2023-09-26	[Ferguson Wellman]	losttrust	Link
2023-09-26	[TORMAX]	losttrust	Link
2023-09-26	[Brown and Streza]	losttrust	Link
2023-09-26	[Bit]	losttrust	Link
2023-09-26	[Glassline]	losttrust	Link
2023-09-26	[SydganCorp]	losttrust	Link
2023-09-26	[Alexander City, Alabama]	losttrust	Link
2023-09-26	[SPEC Engineering]	losttrust	Link
2023-09-26	[Jersey College]	losttrust	Link
2023-09-26	[JSM Group]	losttrust	Link
2023-09-26	[Key Construction]	losttrust	Link
2023-09-26	[Leiblein & Kollegen Steuerberatungsgesellschaft]	losttrust	Link
2023-09-26	[Liberty Lines]	losttrust	Link
2023-09-26	[LoopLoc]	losttrust	Link
2023-09-26	[Reload SPA]	losttrust	Link
2023-09-26	[Ananda Temple]	losttrust	Link
2023-09-26	[Omniatel]	losttrust	Link
2023-09-26	[Paradise Custom Kitchens]	losttrust	Link
2023-09-26	[Specialty Process Equipment]	losttrust	Link
2023-09-26	[The WorkPlace]	losttrust	Link
2023-09-26	[Professional Moving Company - Mackie Group]	losttrust	Link
2023-09-26	[Mexican Government]	losttrust	Link
2023-09-26	[Central Trenching]	losttrust	Link
2023-09-26	[Immanuel Christian School]	losttrust	Link
2023-09-26	[Cullum Services]	losttrust	Link
2023-09-26	[Gold Coin Restaurant]	losttrust	Link
2023-09-26	[Marlboro Township Public School]	losttrust	Link
2023-09-26	[Carmocal]	losttrust	Link
2023-09-26	[Johnson Boiler Works]	losttrust	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-26	[EnCom Polymers]	losttrust	Link
2023-09-26	[Ambrosini Holding]	losttrust	Link
2023-09-26	[Colors Dress]	losttrust	Link
2023-09-26	[THEATER LEAGUE INC]	losttrust	Link
2023-09-26	[GI Medical Services]	losttrust	Link
2023-09-26	[Gordon Law Firm]	losttrust	Link
2023-09-26	[Contraband Control Specialists]	losttrust	Link
2023-09-26	[I&Y Senior Care]	losttrust	Link
2023-09-26	[EWBizservice]	losttrust	Link
2023-09-26	[Center Township Trustee]	losttrust	Link
2023-09-26	[Garlick & Markison]	losttrust	Link
2023-09-26	[Double V Construction]	losttrust	Link
2023-09-26	[Swann's Furniture & Design]	losttrust	Link
2023-09-26	[Gateseven Media Group]	losttrust	Link
2023-09-26	[Asia Vegetable]	losttrust	Link
2023-09-26	[Carnelutti Law Firm]	losttrust	Link
2023-09-26	[Foundation Professionals of Florida]	losttrust	Link
2023-09-26	[WEBBER RESTAURANT GROUP]	8base	Link
2023-09-26	[Pond Security]	alphv	Link
2023-09-26	[SUD TRADING COMPANY]	8base	Link
2023-09-16	[gov.la]	ransomed	Link
2023-09-25	[mango.bg]	ransomed	Link
2023-09-25	[ebag.bg]	ransomed	Link
2023-09-25	[popolo.bg]	ransomed	Link
2023-09-25	[andrews.bg]	ransomed	Link
2023-09-25	[ardes.bg]	ransomed	Link
2023-09-25	[myshoes.bg]	ransomed	Link
2023-09-26	[ecco.bg]	ransomed	Link
2023-09-26	[districtshoes.bg]	ransomed	Link
2023-09-26	[footshop.bg]	ransomed	Link
2023-09-26	[Punto.bg]	ransomed	Link
2023-09-26	[bnm.bg]	ransomed	Link
2023-09-26	[SONY.COM]	ransomed	Link
2023-09-26	[NTT Docomo - Japan 1st Mobile Operator]	ransomed	Link
2023-09-20	[Waterloo Media]	noescape	Link
2023-09-20	[Powerhouse Retail Services LLC]	noescape	Link
2023-09-25	[zzcoldstores.com]	alphv	Link
2023-09-25	[ZZColdstores]	alphv	Link
2023-09-25	[Nusmiles Hospital]	knight	Link
2023-09-25	[Ministry Of Finance (Kuwait)]	rhysida	Link
2023-09-25	[Stratesys Full data leak]	ragnarlocker	Link
2023-09-25	[Praxis Arndt und Langer]	8base	Link
2023-09-25	[PRETZEL-STOUFFER]	alphv	Link
2023-09-25	[J.T. Cullen Co., Inc.]	8base	Link
2023-09-25	[Springer Eubank]	8base	Link
2023-09-24	[MNGI Digestive Health2]	alphv	Link
2023-09-24	[altmanplants.com]	lockbit3	Link
2023-09-17	[Leekes Ltd]	noescape	Link
2023-09-24	[Epson]	stormous	Link
2023-09-24	[Phil-Data Business Systems was hacked. A lot of critical data was stolen. We've gained acc]	alphv	Link
2023-09-23	[Clarion is the most dangerous electronics to use that can cause you to be hacked]	alphv	Link
2023-09-23	[Interep]	stormous	Link
2023-09-16	[BPR Properties LLC]	noescape	Link
2023-09-23	[Franktronics, Inc]	medusa	Link
2023-09-23	[Philippine Health Insurance]	medusa	Link
2023-09-23	[F Hinds]	bianlian	Link
2023-09-23	[FabricATE Engineering]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-23	[The Envelope Works Ltd]	8base	Link
2023-09-23	[Ort Harmelin College of Engineering]	rhysida	Link
2023-09-22	[SMWLLC.COM]	clop	Link
2023-09-22	[marshallindtech.com]	lockbit3	Link
2023-09-22	[precisionpractice.com]	lockbit3	Link
2023-09-22	[Agilitas IT Solutions Limited]	incransom	Link
2023-09-22	[CLX Logistics]	akira	Link
2023-09-22	[Progressive Leasing (40 million Customers PII Data)]	alphv	Link
2023-09-22	[Announcement: COMECA Group going to be Leaked]	ragnarlocker	Link
2023-09-22	[SAGAM Groupe - a company with dozens of vulnerabilities in its network has been hacked and]	alphv	Link
2023-09-22	[Pik Rite]	alphv	Link
2023-09-22	[Announcement: Skatax Accounting company going to be leaked]	ragnarlocker	Link
2023-09-22	[pelmorex.com]	lockbit3	Link
2023-09-22	[Carlo Ditta]	alphv	Link
2023-09-22	[Hospice of Huntington]	karakurt	Link
2023-09-22	[Yusen Logistics]	alphv	Link
2023-09-22	[haciendazorita.com]	threeam	Link
2023-09-22	[fi-tech.com]	threeam	Link
2023-09-22	[Retail House - Full Leak]	ragnarlocker	Link
2023-09-22	[Yakima Valley Radiology]	karakurt	Link
2023-09-22	[neuraxpharm.com]	threeam	Link
2023-09-22	[Holon Institute of Technology]	rhysida	Link
2023-09-22	[PainCare]	alphv	Link
2023-09-22	[TAOGLAS]	alphv	Link
2023-09-22	[Auckland University of Technology]	monti	Link
2023-09-21	[Mole Valley Farmers]	alphv	Link
2023-09-21	[ruko.de]	alphv	Link
2023-09-21	[Unique Engineering is the most collaborative and dangerous construction company in Asia]	alphv	Link
2023-09-21	[Arail]	alphv	Link
2023-09-21	[Cosal is a company that distributes personal and confidential data of its customers and re]	alphv	Link
2023-09-21	[ende.co.ao is a company you can test corporate network hack on and have 100% hacking succe]	alphv	Link
2023-09-21	[Announcement: Stratesys solutions going to be leaked]	ragnarlocker	Link
2023-09-21	[Announcement: Stratesys solutions going to b]	ragnarlocker	Link
2023-09-21	[Road Safety]	bianlian	Link
2023-09-21	[Smartfren Telecom]	bianlian	Link
2023-09-21	[DM Civil]	cactus	Link
2023-09-03	[Hawkins Delafield Wood]	ransomhouse	Link
2023-09-21	[NOVEXCO]	alphv	Link
2023-09-20	[messner.com]	lockbit3	Link
2023-09-10	[IKP]	noescape	Link
2023-09-14	[Kool-Air Inc]	noescape	Link
2023-09-10	[Küng Ag Bern]	noescape	Link
2023-09-20	[Chait]	medusa	Link
2023-09-20	[Gulf American Lines]	medusa	Link
2023-09-20	[hwwealth.com]	lockbit3	Link
2023-09-20	[constantinecannon.com]	lockbit3	Link
2023-09-20	[bauscherhepp.com]	lockbit3	Link
2023-09-20	[compass-inc.com]	lockbit3	Link
2023-09-20	[ENTRUST Solutions Group]	incransom	Link
2023-09-20	[Federal Labor Relations Authority]	incransom	Link
2023-09-20	[Leoch Battery]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-20	[Bacon Universal]	cactus	Link
2023-09-20	[Spuncast]	cactus	Link
2023-09-20	[payrollselectservices.com]	lockbit3	Link
2023-09-20	[Al Ashram Contracting]	alphv	Link
2023-09-20	[University Obrany - Press Release]	monti	Link
2023-09-19	[fersan.com.tr]	lockbit3	Link
2023-09-19	[Announcement: Groupe Fructa Partner will be leaked soon]	ragnarlocker	Link
2023-09-19	[American University of Antigua]	alphv	Link
2023-09-19	[Gossler, Gobert & Wolters Group.]	donutleaks	Link
2023-09-19	[Agilitas IT Solutions Limited]	donutleaks	Link
2023-09-19	[Peacock Bros]	cactus	Link
2023-09-19	[Hacketts printing services]	knight	Link
2023-09-19	[CEFCO]	snatch	Link
2023-09-19	[ZILLI]	snatch	Link
2023-09-19	[Florida Department of Veterans' Affairs]	snatch	Link
2023-09-17	[CITIZEN company LEAKED]	ragnarlocker	Link
2023-09-18	[First Line]	play	Link
2023-09-18	[Rea Magnet Wire]	play	Link
2023-09-18	[RTA]	play	Link
2023-09-18	[TSC]	play	Link
2023-09-18	[PASCHAL - Werk G Maier]	play	Link
2023-09-18	[Vucke]	play	Link
2023-09-18	[Elemetal]	incransom	Link
2023-09-18	[Glovis America]	akira	Link
2023-09-18	[Fuji Seal International (US branch)]	akira	Link
2023-09-18	[Hoteles Xcaret]	blackbyte	Link
2023-09-18	[Agriloja.pt Full Leak]	everest	Link
2023-09-18	[Dustin J Will LCC / Dustin J Will Sole MBR]	knight	Link
2023-09-18	[Lopez & Associates Inc]	knight	Link
2023-09-18	[Auckland Transport]	medusa	Link
2023-09-18	[Araújo e Policastro Advogados]	8base	Link
2023-09-17	[Announcement: Retail House going to be LEAKED]	ragnarlocker	Link
2023-09-17	[Delta Group]	8base	Link
2023-09-16	[TransTerra]	ciphbit	Link
2023-09-16	[Marston Domsel]	ciphbit	Link
2023-09-16	[tuvsud.com]	lockbit3	Link
2023-09-16	[perfectlaw.com]	lockbit3	Link
2023-09-16	[beamconstruction.com]	lockbit3	Link
2023-09-16	[scottpartners.com]	lockbit3	Link
2023-09-16	[eljayoil.com]	lockbit3	Link
2023-09-16	[dasholding.ae]	lockbit3	Link
2023-09-16	[faithfamilyacademy.org]	lockbit3	Link
2023-09-16	[syntech.com.sg]	lockbit3	Link
2023-09-16	[piramidal.com.br]	lockbit3	Link
2023-09-16	[tlip2.com]	lockbit3	Link
2023-09-16	[energyinsight.co.za]	lockbit3	Link
2023-09-16	[mehmetceylanyapi.com.tr]	lockbit3	Link
2023-09-16	[aeroportlleida.cat]	lockbit3	Link
2023-09-16	[lamaisonmercier.com]	lockbit3	Link
2023-09-16	[neolaser.es]	lockbit3	Link
2023-09-16	[commercialfluidpower.com]	lockbit3	Link
2023-09-16	[glat.zapweb.co.il]	lockbit3	Link
2023-09-16	[motsaot.co.il]	lockbit3	Link
2023-09-16	[gsaenz.com.mx]	lockbit3	Link
2023-09-16	[ipsenlogistics.com]	lockbit3	Link
2023-09-16	[Financial Decisions]	alphv	Link
2023-09-15	[Updates: Israel "MYMC"]	ragnarlocker	Link
2023-09-15	[hollandspecial]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-15	[pelicanwoodcliff.com]	lockbit3	Link
2023-09-15	[hillsboroughschools.org]	lockbit3	Link
2023-09-15	[Steelforce]	trigona	Link
2023-09-14	[wdgroup.com.my]	threeam	Link
2023-09-14	[pvbfabs.com]	threeam	Link
2023-09-14	[intechims.com]	threeam	Link
2023-09-14	[zero-pointorganics.com]	threeam	Link
2023-09-14	[visitingphysiciansnetwork.com]	threeam	Link
2023-09-14	[clearwaterlandscape.com]	threeam	Link
2023-09-14	[Statement on MGM Resorts International: Setting the record straight]	alphv	Link
2023-09-14	[etsi.uy]	knight	Link
2023-09-14	[Ja Quith Press Release]	monti	Link
2023-09-14	[East Baking Press Release]	monti	Link
2023-09-14	[American Steel & Aluminum]	akira	Link
2023-09-14	[Waterford Retirement Residence]	ciphbit	Link
2023-09-14	[Shelly Engineering Metal Work]	ciphbit	Link
2023-09-14	[Harmonic Accounting]	ciphbit	Link
2023-09-14	[Imperador S.R.L]	ciphbit	Link
2023-09-14	[Waterford Retirement Residence]	ciphbit	Link
2023-09-14	[Shelly Engineering Metal Work]	ciphbit	Link
2023-09-14	[RSV Centrale Bvba]	ciphbit	Link
2023-09-14	[Soprovise]	ciphbit	Link
2023-09-14	[carthagehospital.com]	lockbit3	Link
2023-09-07	[Fondation Vincent De Paul]	noescape	Link
2023-09-07	[EDUCAL, SA de CV]	noescape	Link
2023-09-13	[Enpos]	stormous	Link
2023-09-13	[clearcreek.org]	lockbit3	Link
2023-09-13	[Financial Services Commission]	blacksuit	Link
2023-09-13	[Cedar Holdings]	trigona	Link
2023-09-13	[Benefit Management INC]	knight	Link
2023-09-13	[Dpc & S]	play	Link
2023-09-13	[Carpet One]	play	Link
2023-09-13	[Markentrainer Werbeagentur, Elwema Automotive]	play	Link
2023-09-13	[Tanachira Group]	knight	Link
2023-09-12	[Accuride]	akira	Link
2023-09-12	[Abbeyfield]	incransom	Link
2023-09-12	[Morgan Smith Industries LLC]	knight	Link
2023-09-12	[Decarie Motors Inc]	knight	Link
2023-09-12	[sinloc.com]	lockbit3	Link
2023-09-12	[M-Extend / MANIP]	alphv	Link
2023-09-12	[Dee Sign]	lorenz	Link
2023-09-12	[Credifiel was hacked and a lot of personal customer and financial information was stolen]	alphv	Link
2023-09-12	[Derrimon Trading was hacked. Critical data of the company and its customers was stolen]	alphv	Link
2023-09-12	[CORTEL Technologies]	qilin	Link
2023-09-11	[Alps Alpine]	blackbyte	Link
2023-09-11	[24/7 Express Logistics (Unpay-Start Leaking)]	ragroup	Link
2023-09-07	[International Joint Commission]	noescape	Link
2023-09-02	[Altmann Dental GmbH & Co KG]	noescape	Link
2023-09-03	[AdSage Technology Co., Ltd.]	noescape	Link
2023-09-11	[deeroaks.com]	lockbit3	Link
2023-09-11	[Cmranallolaw.com]	everest	Link
2023-09-11	[Wardlaw Claims Service]	cactus	Link
2023-09-11	[Levine Bagade Han]	cactus	Link
2023-09-11	[Leekes]	cactus	Link
2023-09-11	[My Insurance Broker]	cactus	Link
2023-09-11	[Unimarketing]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-11	[cfsigroup.ca]	lockbit3	Link
2023-09-11	[Wave Hill]	medusa	Link
2023-09-11	[Steripharma]	medusa	Link
2023-09-11	[co.grant.mn.us]	lockbit3	Link
2023-09-11	[KUITS Solicitors]	alphv	Link
2023-09-11	[Ford Covesa]	8base	Link
2023-09-10	[New Venture Escrow]	bianlian	Link
2023-09-10	[BOZOVICH TIMBER PRODUCTS INC]	mallox	Link
2023-09-10	[njsba.com]	abyss	Link
2023-09-10	[Singing River Health System]	rhysida	Link
2023-09-10	[Core Desktop]	rhysida	Link
2023-09-09	[Kirby Risk]	blackbyte	Link
2023-09-09	[airelec.bg]	ransomed	Link
2023-09-09	[pilini.bg]	ransomed	Link
2023-09-09	[kasida.bg]	ransomed	Link
2023-09-09	[proxy-sale.com]	ransomed	Link
2023-09-09	[IT-Center Syd]	rhysida	Link
2023-09-08	[www.northriverco.com]	abyss	Link
2023-09-08	[sd69.org]	lockbit3	Link
2023-09-08	[milbermakris.com]	lockbit3	Link
2023-09-08	[monaco-technologies.com]	lockbit3	Link
2023-09-08	[UNIVERSAL REALTY GROUP]	8base	Link
2023-09-08	[Geo Tek]	cactus	Link
2023-09-08	[hanwha.com]	lockbit3	Link
2023-09-08	[Custom Powder Systems]	cactus	Link
2023-09-08	[JSS Almonds]	cactus	Link
2023-09-08	[atWork Office Furniture]	cactus	Link
2023-09-08	[BRiC Partnership]	cactus	Link
2023-09-08	[PAUL-ALEXANDRE DOICESCO]	qilin	Link
2023-09-08	[WACOAL]	qilin	Link
2023-09-08	[Linktera]	ransomed	Link
2023-09-07	[24/7 Express Logistics]	ragroup	Link
2023-09-07	[FOCUS Business Solutions]	blackbyte	Link
2023-09-07	[Chambersburg Area School District]	blackbyte	Link
2023-09-07	[Pvc-ms]	stormous	Link
2023-09-07	[toua.net]	lockbit3	Link
2023-09-07	[Conselho Superior da Justiça do Trabalho]	8base	Link
2023-09-07	[Sebata Holdings (MICROmega Holdings)]	bianlian	Link
2023-09-07	[TORMAX USA]	cactus	Link
2023-09-07	[West Craft Manufacturing]	cactus	Link
2023-09-07	[Trimaran Capital Partners]	cactus	Link
2023-09-07	[Specialised Management Services]	cactus	Link
2023-09-06	[nobleweb.com]	lockbit3	Link
2023-09-06	[protosign.it]	lockbit3	Link
2023-09-06	[concrejato.com.br]	lockbit3	Link
2023-09-06	[meroso.be]	lockbit3	Link
2023-09-06	[qsoftnet.com]	lockbit3	Link
2023-09-06	[ragasa.com.mx]	lockbit3	Link
2023-09-06	[I Keating Furniture World]	incransom	Link
2023-09-06	[onyx-fire.com]	lockbit3	Link
2023-09-06	[gormanusa.com]	lockbit3	Link
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	Link
2023-09-06	[It4 Solutions Robras]	incransom	Link
2023-09-06	[Smead]	blackbyte	Link
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	Link
2023-09-06	[Ayass BioScience]	alphv	Link
2023-09-06	[Sabre Corporation]	dunghill_leak	Link
2023-09-06	[Energy One]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	Link
2023-09-06	[Chula Vista Electric (CVE)]	8base	Link
2023-09-05	[Precisely, Winshuttle]	play	Link
2023-09-05	[Kikkerland Design]	play	Link
2023-09-05	[Markentrainer Werbeagentur]	play	Link
2023-09-05	[Master Interiors]	play	Link
2023-09-05	[Bordelon Marine]	play	Link
2023-09-05	[Majestic Spice]	play	Link
2023-09-04	[Infinity Construction Company]	noescape	Link
2023-09-05	[Maxxd Trailers]	cactus	Link
2023-09-05	[MINEMAN Systems]	cactus	Link
2023-09-05	[Promotrans]	cactus	Link
2023-09-05	[Seymours]	cactus	Link
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	Link
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	Link
2023-09-05	[Marfrig Global Foods]	cactus	Link
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	Link
2023-09-05	[Barry Plant LEAK!]	alphv	Link
2023-09-05	[Barsco]	cactus	Link
2023-09-05	[Foroni SPA]	cactus	Link
2023-09-05	[Hornsyld Købmandsgaard]	cactus	Link
2023-09-05	[Lagarde Meregnani]	cactus	Link
2023-09-05	[spmblaw.com]	lockbit3	Link
2023-09-05	[Unimed]	trigona	Link
2023-09-05	[Cyberport]	trigona	Link
2023-09-05	[godbeylaw.com]	lockbit3	Link
2023-09-01	[Firmdale Hotels]	play	Link
2023-09-04	[easydentalcare.us]	ransomed	Link
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
2023-09-04	[makflix.eu]	ransomed	Link
2023-09-04	[nucleus.live]	ransomed	Link
2023-09-04	[wantager.com]	ransomed	Link
2023-09-04	[Zurvita]	ragroup	Link
2023-09-04	[Piex Group]	ragroup	Link
2023-09-04	[Yuxin Automobile Co.Ltd ( )]	ragroup	Link
2023-09-02	[Mulkay Cardiology Consultants]	noescape	Link
2023-09-04	[Balcan]	cactus	Link
2023-09-04	[Barco Uniforms]	cactus	Link
2023-09-04	[Swipe.bg]	ransomed	Link
2023-09-04	[Balmit Bulgaria]	ransomed	Link
2023-09-04	[cdwg.com]	lockbit3	Link
2023-09-04	[Betton France]	medusa	Link
2023-09-04	[Jules B]	medusa	Link
2023-09-04	[VVandA]	8base	Link
2023-09-04	[Prodegest Assessors]	8base	Link
2023-09-04	[Knight Barry Title]	snatch	Link
2023-09-03	[phms.com.au]	ransomed	Link
2023-09-03	[paynesvilleareainsurance.com]	ransomed	Link
2023-09-03	[SKF.com]	ransomed	Link
2023-09-03	[gosslaw.com]	lockbit3	Link
2023-09-03	[marianoshoes.com]	lockbit3	Link
2023-09-03	[Arkopharma]	incransom	Link
2023-09-02	[Taylor University]	moneymessage	Link
2023-09-03	[Riverside Logistics]	moneymessage	Link
2023-09-03	[Estes Design & Manufacturing]	moneymessage	Link
2023-09-03	[Aiphone]	moneymessage	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	rancoz	Link
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	rancoz	Link
2023-09-03	[Newton Media A.S]	alphv	Link
2023-09-03	[Lawsonlundell]	alphv	Link
2023-09-02	[glprop.com]	lockbit3	Link
2023-09-02	[Strata Plan Australia]	alphv	Link
2023-09-02	[TissuPath Australia]	alphv	Link
2023-09-02	[seasonsdarlingharbour.com.au]	lockbit3	Link
2023-09-02	[nerolac.com]	lockbit3	Link
2023-09-02	[ramlowstein.com]	lockbit3	Link
2023-09-02	[Barry Plant Real Estate Australia]	alphv	Link
2023-09-02	[sterncoengineers.com]	lockbit3	Link
2023-09-02	[attorneydanwinder.com]	lockbit3	Link
2023-09-02	[designlink.us]	lockbit3	Link
2023-09-02	[gh2.com]	lockbit3	Link
2023-09-02	[DOIT - Canadian IT company allowed leak of its own clients.]	ragnarlocker	Link
2023-09-02	[SKF.com]	everest	Link
2023-09-02	[Powersportsmarketing.com]	everest	Link
2023-09-02	[Statefarm.com]	everest	Link
2023-09-02	[Aban Tether & OK exchange]	arvinclub	Link
2023-09-02	[cc-gorgesardeche.fr]	lockbit3	Link
2023-09-01	[cciamp.com]	lockbit3	Link
2023-09-01	[Templeman Consulting Group Inc]	bianlian	Link
2023-09-01	[vodatech.com.tr]	lockbit3	Link
2023-09-01	[F???????? ?????s]	play	Link
2023-09-01	[Hawaii Health System]	ransomed	Link
2023-09-01	[hamilton-techservices.com]	lockbit3	Link
2023-09-01	[aquinas.qld.edu.au]	lockbit3	Link
2023-09-01	[konkconsulting.com]	lockbit3	Link
2023-09-01	[Piex Group]	ragroup	Link
2023-09-01	[Yuxin Automobile Co.Ltd( )]	ragroup	Link

Quellen

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

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.