Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240314

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

Fortinet-Patchday: Updates gegen kritische Schwachstellen

Fortinet hat zum März-Patchday Sicherheitslücken in FortiOS, FortiProxy, FortiClientEMS und im FortiManager geschlossen.

- Link

—

Adobe-Patchday: Angreifer können verwundbare Systeme übernehmen

Adobe stopft am März-Patchday teils kritische Sicherheitslücken in sechs Produkten. Sie erlauben unter anderem Codeschmuggel.

- Link

—

Microsoft Patchday: Hersteller stopft 59 Sicherheitslücken

Der März-Patchday von Microsoft ist etwas weniger umfangreich: 59 Sicherheitslecks haben die Entwickler gestopft.

- Link

—

Google Chrome: Lücke erlaubte Codeschmuggel

Google schließt drei Sicherheitslücken im Webbrowser Chrome. Mindestens eine gilt als hochriskant, Angreifer könnten Schadcode dadurch einschleusen.

- Link

—

Synology: Update schließt “wichtige” Lücken in Synology Router Manager

Im Synology Router Manager (SRM) klaffen Sicherheitslecks, durch die Angreifer etwa Scripte einschleusen können. Ein Update steht bereit.

- Link

—

SAP schließt zehn Sicherheitslücken am März-Patchday

SAP hat zehn neue Sicherheitsmitteilungen zum März-Patchday veröffentlicht. Zwei der geschlossenen Lücken gelten als kritisch.

- Link

—

ArubaOS: Sicherheitslücken erlauben Befehlsschmuggel

HPE Aruba hat eine Sicherheitsmitteilung zu mehreren Lücken herausgegeben. Angreifer können Befehle einschleusen oder einen DoS auslösen.

- Link

—

Qnap hat teils kritische Lücken in seinen Betriebssystemen geschlossen

Qnap hat Warnungen vor Sicherheitslücken in QTS, QuTS Hero und QuTScloud veröffentlicht. Aktualisierte Firmware dichtet sie ab.

- Link

—

Jetzt patchen! Deutschland führt Liste mit verwundbaren TeamCity-Systemen an

Angreifer kompromittieren derzeit gehäuft das Software-Distributionssystem TeamCity. Das kann ein Ausgangspunkt für eine Supply-Chain-Attacke sein.

- Link

—

Cisco: Angreifer können sich zum Root-Nutzer unter Linux machen

Die Softwareentwickler des Netzwerkausrüsters Cisco haben mehrere Sicherheitslücken geschlossen.

- 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	0.901600000	0.987150000	Link
CVE-2023-6553	0.916210000	0.988330000	Link
CVE-2023-5360	0.967230000	0.996330000	Link
CVE-2023-4966	0.963970000	0.995280000	Link
CVE-2023-47246	0.943540000	0.991440000	Link
CVE-2023-46805	0.962740000	0.994890000	Link
CVE-2023-46747	0.972020000	0.998040000	Link
CVE-2023-46604	0.972730000	0.998390000	Link
CVE-2023-43177	0.927670000	0.989600000	Link
CVE-2023-42793	0.973450000	0.998840000	Link
CVE-2023-39143	0.933560000	0.990210000	Link
CVE-2023-38646	0.916640000	0.988380000	Link
CVE-2023-38205	0.934710000	0.990320000	Link
CVE-2023-38203	0.959860000	0.994270000	Link
CVE-2023-38035	0.972370000	0.998260000	Link
CVE-2023-36845	0.966580000	0.996110000	Link
CVE-2023-3519	0.911860000	0.987960000	Link
CVE-2023-35082	0.935540000	0.990400000	Link
CVE-2023-35078	0.963380000	0.995090000	Link
CVE-2023-34960	0.929930000	0.989780000	Link
CVE-2023-34634	0.919000000	0.988630000	Link
CVE-2023-34362	0.959040000	0.994050000	Link
CVE-2023-34039	0.901300000	0.987120000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.904650000	0.987340000	Link
CVE-2023-33246	0.973410000	0.998800000	Link
CVE-2023-32315	0.973840000	0.999040000	Link
CVE-2023-32235	0.905760000	0.987420000	Link
CVE-2023-30625	0.946250000	0.991800000	Link
CVE-2023-30013	0.945460000	0.991700000	Link
CVE-2023-29300	0.963690000	0.995190000	Link
CVE-2023-29298	0.921360000	0.988840000	Link
CVE-2023-28771	0.923800000	0.989140000	Link
CVE-2023-28432	0.941310000	0.991080000	Link
CVE-2023-28121	0.929770000	0.989740000	Link
CVE-2023-27524	0.972240000	0.998190000	Link
CVE-2023-27372	0.971320000	0.997750000	Link
CVE-2023-27350	0.971970000	0.998020000	Link
CVE-2023-26469	0.937680000	0.990660000	Link
CVE-2023-26360	0.960730000	0.994520000	Link
CVE-2023-26035	0.970030000	0.997180000	Link
CVE-2023-25717	0.962180000	0.994760000	Link
CVE-2023-2479	0.962540000	0.994840000	Link
CVE-2023-24489	0.973400000	0.998790000	Link
CVE-2023-23752	0.948570000	0.992210000	Link
CVE-2023-23397	0.917330000	0.988450000	Link
CVE-2023-22527	0.965680000	0.995900000	Link
CVE-2023-22518	0.970110000	0.997210000	Link
CVE-2023-22515	0.972700000	0.998380000	Link
CVE-2023-21839	0.960490000	0.994470000	Link
CVE-2023-21554	0.959700000	0.994230000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-20887	0.965070000	0.995660000	Link
CVE-2023-20198	0.919220000	0.988640000	Link
CVE-2023-1671	0.964380000	0.995420000	Link
CVE-2023-0669	0.968640000	0.996760000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 13 Mar 2024

[UPDATE] [hoch] Android Patchday Juni 2022

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand auszulösen.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Wed, 13 Mar 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

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft Exchange Server: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft Exchange Server 2016 und Microsoft Exchange Server 2019 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft System Center: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft System Center ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und seine Rechte zu erweitern.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Infor mationen offenzulegen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft SQL Server (MSSQL): Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Microsoft SQL Server (MSSQL) ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Fortinet FortiOS und FortiProxy: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Fortinet FortiOS und Fortinet FortiProxy ausnutzen, um beliebigen Code auszuführen, seine Privilegien zu erweitern oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft Apps: Mehrere Schwachstellen

Ein Angreifer kann eine Schwachstelle in Microsoft Outlook for Android, Microsoft Skype, Microsoft Authenticator und Microsoft Intune Company Portal for Android ausnutzen, um beliebigen Code auszuführen, seine Berechtigungen zu erweitern oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 13 Mar 2024

[NEU] [kritisch] Microsoft Azure: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und Informationen falsch darzustellen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Microsoft Visual Studio 2022: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um einen Denial of Service Angriff durchzuführen oder seine Privilegien zu erweitern.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Adobe Creative Cloud: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Adobe Creative Cloud Apps ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Nvidia Treiber ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Fortinet FortiClientEMS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Fortinet FortiClient ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

[NEU] [hoch] Fortinet FortiAnalyzer und Fortinet FortiManager: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Fortinet FortiAnalyzer und Fortinet FortiManager ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 13 Mar 2024

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

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

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/14/2024	[EulerOS Virtualization 2.10.0 : binutils (EulerOS-SA-2024-1375)]	critical
3/14/2024	[EulerOS Virtualization 2.10.1 : curl (EulerOS-SA-2024-1355)]	critical
3/14/2024	[EulerOS Virtualization 2.10.1 : kernel (EulerOS-SA-2024-1360)]	critical
3/14/2024	[EulerOS Virtualization 2.10.0 : zlib (EulerOS-SA-2024-1394)]	critical
3/14/2024	[EulerOS Virtualization 2.10.0 : kernel (EulerOS-SA-2024-1381)]	critical
3/14/2024	[EulerOS Virtualization 2.10.1 : zlib (EulerOS-SA-2024-1373)]	critical
3/14/2024	[EulerOS Virtualization 2.10.1 : binutils (EulerOS-SA-2024-1354)]	critical
3/14/2024	[EulerOS Virtualization 2.10.0 : curl (EulerOS-SA-2024-1376)]	critical
3/13/2024	[Slackware Linux 15.0 / current expat Vulnerability (SSA:2024-073-01)]	critical
3/13/2024	[Ubuntu 14.04 LTS : X.Org X Server vulnerabilities (USN-6587-5)]	critical
3/14/2024	[EulerOS Virtualization 2.10.1 : grub2 (EulerOS-SA-2024-1358)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : python-pillow (EulerOS-SA-2024-1389)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : libX11 (EulerOS-SA-2024-1362)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : vim (EulerOS-SA-2024-1372)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : nghttp2 (EulerOS-SA-2024-1386)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : python-pillow (EulerOS-SA-2024-1368)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : vim (EulerOS-SA-2024-1393)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : grub2 (EulerOS-SA-2024-1379)]	high

Datum	Schwachstelle	Bewertung
3/14/2024	[EulerOS Virtualization 2.10.0 : httpd (EulerOS-SA-2024-1380)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : nghttp2 (EulerOS-SA-2024-1365)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : httpd (EulerOS-SA-2024-1359)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : libX11 (EulerOS-SA-2024-1383)]	high
3/14/2024	[EulerOS Virtualization 2.10.1 : python-urllib3 (EulerOS-SA-2024-1369)]	high
3/14/2024	[EulerOS Virtualization 2.10.0 : python-urllib3 (EulerOS-SA-2024-1390)]	high
3/13/2024	[Fedora 38 : thunderbird (2024-325c1d1fce)]	high
3/13/2024	[Fedora 39 : chromium (2024-99d177633f)]	high
3/13/2024	[Fedora 39 : python-fastapi / python-multipart (2024-2e802cdb4b)]	high
3/13/2024	[Fedora 38 : python-fastapi / python-multipart (2024-09c7f715c9)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 13 Mar 2024

Stealing Part Of A Production Language Model

In this whitepaper, the authors introduce the first model-stealing attack that extracts precise, nontrivial information from black-box production language models like OpenAI’s ChatGPT or Google’s PaLM-2. Specifically, their attack recovers the embedding projection layer (up to symmetries) of a transformer model, given typical API access. For under $20 USD, their attack extracts the entire projection matrix of OpenAI’s ada and babbage language models. They thereby confirm, for the first time, that these black-box models have a hidden dimension of 1024 and 2048, respectively. They also recover the exact hidden dimension size of the gpt-3.5-turbo model, and estimate it would cost under $2,000 in queries

to recover the entire projection matrix. They conclude with potential defenses and mitigations, and discuss the implications of possible future work that could extend this attack.

- Link

—

” “Wed, 13 Mar 2024

Client Details System 1.0 SQL Injection

Client Details System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 13 Mar 2024

MetaFox 5.1.8 Shell Upload

MetaFox versions 5.1.8 and below suffer from a remote shell upload vulnerability.

- Link

—

” “Wed, 13 Mar 2024

Cisco Firepower Management Center Remote Command Execution

Cisco Firepower Management Center suffers from an authenticated remote command execution vulnerability. Many versions spanning the 7.x.x.x and 6.x.x.x branches are affected.

- Link

—

” “Wed, 13 Mar 2024

SnipeIT 6.2.1 Cross Site Scripting

SnipeIT version 6.2.1 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 13 Mar 2024

MSMS-PHP 1.0 Shell Upload

MSMS-PHP version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 13 Mar 2024

MSMS-PHP 1.0 SQL Injection

MSMS-PHP version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 13 Mar 2024

VMware Cloud Director 10.5 Authentication Bypass

VMware Cloud Director version 10.5 suffers from an authentication bypass vulnerability.

- Link

—

” “Wed, 13 Mar 2024

Karaf 4.4.3 Remote Code Execution

Karaf version 4.4.3 suffers from a remote code execution vulnerability.

- Link

—

” “Wed, 13 Mar 2024

OSGi 3.7.2 Remote Code Execution

OSGi versions 3.7.2 and below suffer from a remote code execution vulnerability.

- Link

—

” “Wed, 13 Mar 2024

OSGi 3.18 Remote Code Execution

OSGi versions 3.8 through 3.18 suffer from a remote code execution vulnerability.

- Link

—

” “Tue, 12 Mar 2024

NorthStar C2 Agent 1.0 Cross Site Scripting / Remote Command Execution

NorthStar C2 agent version 1.0 applies insufficient sanitization on agent registration routes, allowing an unauthenticated attacker to send multiple malicious agent registration requests to the teamserver to incrementally build a functioning javascript payload in the logs web page. This cross site scripting payload can be leveraged to execute commands on NorthStar C2 agents.

- Link

—

” “Tue, 12 Mar 2024

Human Resource Management System 1.0 SQL Injection

Human Resource Management System version 1.0 suffers from a remote SQL injection vulnerability. Original discovery of SQL injection in this version is attributed to Abdulhakim Oner in March of 2023.

- Link

—

” “Mon, 11 Mar 2024

Numbas Remote Code Execution

Numbas versions prior to 7.3 suffer from a remote code execution vulnerability.

- Link

—

” “Mon, 11 Mar 2024

Sitecore 8.2 Remote Code Execution

Sitecore version 8.2 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 11 Mar 2024

Adobe ColdFusion 2018,15 / 2021,5 Arbitrary File Read

Adobe ColdFusion versions 2018,15 and below and versions 2021,5 and below suffer from an arbitrary file read vulnerability.

- Link

—

” “Mon, 11 Mar 2024

Backdoor.Win32.Beastdoor.oq MVID-2024-0674 Remote Command Execution

Backdoor.Win32.Beastdoor.oq malware suffers from a remote command execution vulnerability.

- Link

—

” “Mon, 11 Mar 2024

WordPress Duplicator Data Exposure / Account Takeover

WordPress Duplicator plugin versions prior to 1.5.7.1 suffer from an unauthenticated sensitive data exposure vulnerability that can lead to account takeover.

- Link

—

” “Mon, 11 Mar 2024

RUPPEINVOICE 1.0 SQL Injection

RUPPEINVOICE version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 11 Mar 2024

WordPress Hide My WP SQL Injection

WordPress Hide My WP plugin versions 6.2.9 and below suffer from an unauthenticated remote SQL injection vulnerability.

- Link

—

” “Mon, 11 Mar 2024

DataCube3 1.0 Shell Upload

DataCube3 version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 11 Mar 2024

Akaunting 3.1.3 Remote Command Execution

Akaunting versions 3.1.3 and below suffer from a remote command execution vulnerability.
- Link
—
” “Mon, 11 Mar 2024
Hitachi NAS SMU Backup And Restore Insecure Direct Object Reference
Hitachi NAS SMU Backup and Restore versions prior to 14.8.7825.01 suffer from an insecure direct object reference vulnerability.
- Link
—
” “Mon, 11 Mar 2024
TP-Link TL-WR740N Buffer Overflow / Denial Of Service
There exists a buffer overflow vulnerability in the TP-Link TL-WR740 router that can allow an attacker to crash the web server running on the router by sending a crafted request.
- Link
—
” “Fri, 08 Mar 2024
MongoDB 2.0.1 / 2.1.1 / 2.1.4 / 2.1.5 Local Password Disclosure
MongoDB versions 2.0.1, 2.1.1, 2.1.4, and 2.1.5 appear to suffer from multiple localized password disclosure issues.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Wed, 13 Mar 2024
ZDI-24-294: Microsoft Office Performance Monitor Link Following Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 13 Mar 2024
ZDI-24-293: Microsoft Skype Protection Mechanism Failure Remote Code Execution Vulnerability
- Link
—
” “Wed, 13 Mar 2024
ZDI-24-292: Adobe Premiere Pro AVI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link

—

” “Wed, 13 Mar 2024

ZDI-24-291: Adobe Bridge PS File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-290: NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-289: NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-288: NI LabVIEW VI File Parsing Out-of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-287: NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-286: NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 12 Mar 2024

ZDI-24-285: NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-284: Adobe Acrobat Reader DC PDF File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-283: Apple macOS JP2 Image Parsing Uninitialized Pointer Information Disclosure Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-282: Dassault Systèmes eDrawings Viewer SAT File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-281: Dassault Systèmes eDrawings Viewer SAT File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-280: Dassault Systèmes eDrawings Viewer SAT File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-279: Dassault Systèmes eDrawings Viewer SAT File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-278: Dassault Systèmes eDrawings Viewer JT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-277: Dassault Systèmes eDrawings Viewer SAT File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-276: Dassault Systèmes eDrawings Viewer JT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-275: Dassault Systèmes eDrawings Viewer JT File Parsing Out-Of-Bounds Write Remote

Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-274: Dassault Systèmes eDrawings Viewer STL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-273: Dassault Systèmes eDrawings IPT File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-272: Dassault Systèmes eDrawings SAT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-271: Dassault Systèmes eDrawings SAT File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-270: Dassault Systèmes eDrawings STP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-269: Dassault Systèmes eDrawings JT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-268: Dassault Systèmes eDrawings IPT File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-267: Dassault Systèmes eDrawings SLDDRW File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-266: Dassault Systèmes eDrawings IPT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-265: Dassault Systèmes eDrawings SAT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-264: Dassault Systèmes eDrawings IPT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-263: Dassault Systèmes eDrawings SAT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-262: Dassault Systèmes eDrawings JT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-261: Dassault Systèmes eDrawings SLDPRT File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-260: Dassault Systèmes eDrawings IPT File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-259: Dassault Systèmes eDrawings IPT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-258: Dassault Systèmes eDrawings CATPART File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 11 Mar 2024

ZDI-24-257: Dassault Systèmes eDrawings X_B File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

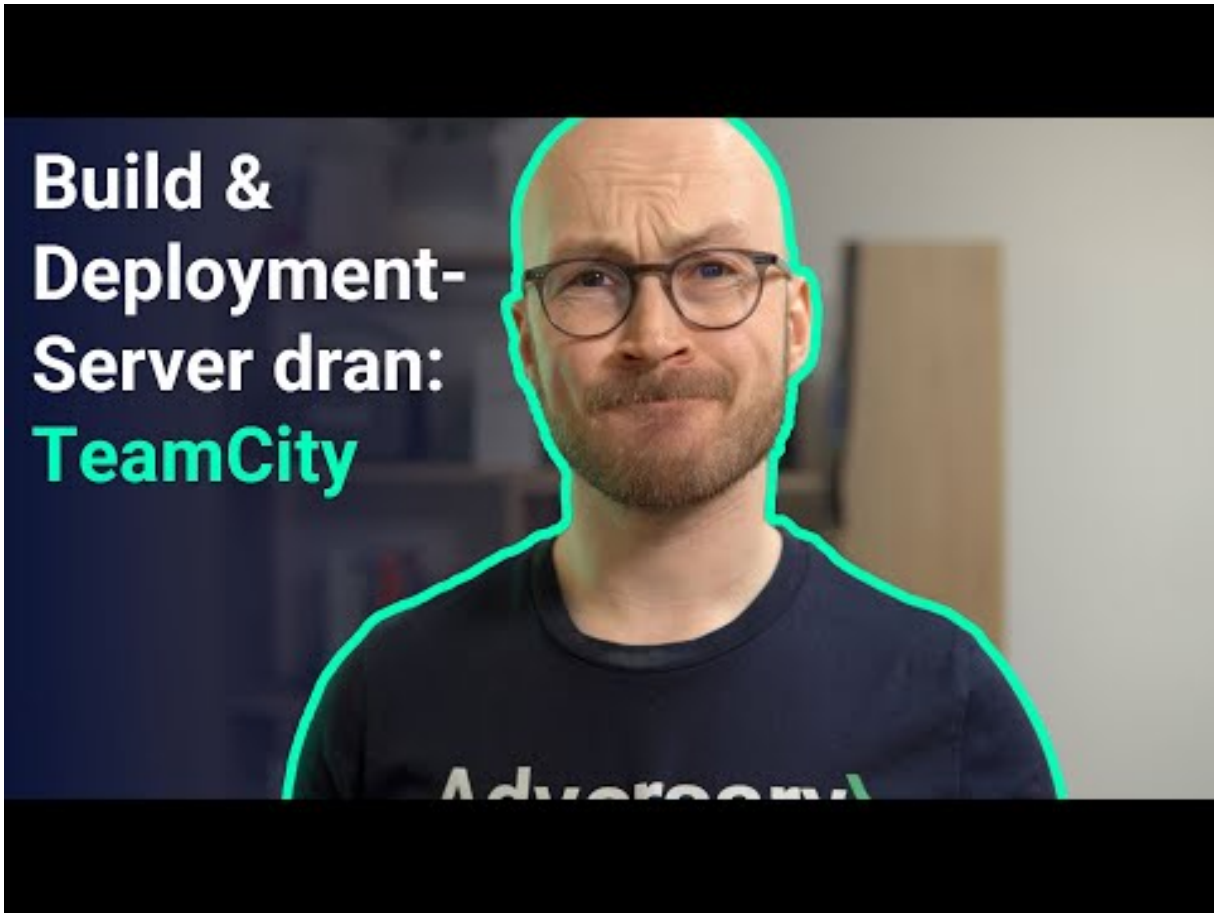
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Hättest du diese Lücke gefunden?



Zum Youtube Video

6 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2024-03-13	Maxis	[MYS]	Link
2024-03-10	edpnet	[BEL]	Link
2024-03-10	Town of Huntsville	[CAN]	Link
2024-03-10	MarineMax	[USA]	Link
2024-03-09	Leicester City Council	[GBR]	Link
2024-03-08	Kärntner Landesversicherung (KLV)	[AUT]	Link
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	Link
2024-03-07	Beyers Koffie	[BEL]	Link
2024-03-06	Brasserie Duvel Moortgat	[BEL]	Link
2024-03-06	Nisqually Red Wind Casino	[USA]	Link
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-04	South St. Paul Public Schools	[USA]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-13	[McKim & Creed]	ransomhub	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Summit Almonds]	akira	Link
2024-03-13	[Encina Wastewater Authority]	blackbyte	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Felda Global Ventures Holdings Berhad]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-13	[geruestbau.com]	lockbit3	Link
2024-03-13	[Judge Rotenberg Center]	blacksuit	Link
2024-03-12	[Dörr Group]	snatch	Link
2024-03-13	[Kovra]	ransomhub	Link
2024-03-13	[Brewer Davidson]	8base	Link
2024-03-13	[Forstinger Österreich GmbH]	8base	Link
2024-03-04	[vsexshop.ru]	werewolves	Link
2024-03-11	[QEO Group]	play	Link
2024-03-12	[ATL]	hunters	Link
2024-03-12	[duvel.com	boulevard.com]	blackbasta
2024-03-11	[Kenneth Young Center]	medusa	Link
2024-03-12	[sunholdings.net]	lockbit3	Link
2024-03-12	[xcelbrands.com]	blackbasta	Link
2024-03-12	[cpacsystems.se]	blackbasta	Link
2024-03-12	[elmatic.de]	blackbasta	Link
2024-03-12	[keystonetech.com]	blackbasta	Link
2024-03-12	[dutyfreeamericas.com]	blackbasta	Link
2024-03-12	[sierralobo.com]	blackbasta	Link
2024-03-12	[contechs.co.uk]	blackbasta	Link
2024-03-12	[creativeenvironments.com]	blackbasta	Link
2024-03-12	[linksunlimited.com]	blackbasta	Link
2024-03-12	[imperialtrading.com]	blackbasta	Link
2024-03-12	[Brooks Tropicals]	rhysida	Link
2024-03-12	[Withall]	blacksuit	Link
2024-03-12	[WALKERSANDFORD]	blacksuit	Link
2024-03-12	[Kaplan]	hunters	Link
2024-03-06	[Sprimoglass]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-11	[Schokinag]	play	Link
2024-03-11	[Zips Car Wash]	play	Link
2024-03-11	[Bechtold]	play	Link
2024-03-11	[Canada Revenue Agency]	play	Link
2024-03-11	[White Oak Partners]	play	Link
2024-03-11	[Ruda Auto]	play	Link
2024-03-11	[Image Pointe]	play	Link
2024-03-11	[Grassmid Transport]	play	Link
2024-03-11	[Fashion UK]	play	Link
2024-03-11	[QI Group]	play	Link
2024-03-11	[BiTec]	play	Link
2024-03-11	[Bridger Insurance]	play	Link
2024-03-11	[SREE Hotels]	play	Link
2024-03-11	[Q?? ??o??]	play	Link
2024-03-11	[Premier Technology]	play	Link
2024-03-11	[londonvisionclinic.com]	lockbit3	Link
2024-03-11	[lec-london.uk]	lockbit3	Link
2024-03-11	[Computan]	ransomhub	Link
2024-03-11	[plymouth.com]	cactus	Link
2024-03-11	[neigc.com]	abyss	Link
2024-03-11	[gpaa.gov.za]	lockbit3	Link
2024-03-11	[NetVigour]	hunters	Link
2024-03-11	[cleshar.co.uk]	cactus	Link
2024-03-11	[ammega.com]	cactus	Link
2024-03-11	[renypicot.es]	cactus	Link
2024-03-11	[Scadea Solutions]	ransomhub	Link
2024-03-09	[https://www.consorzioinnova.it]	alphalocker	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-09	[DVT]	ransomhub	Link
2024-03-09	[Rekamy]	ransomhub	Link
2024-03-09	[go4kora]	ransomhub	Link
2024-03-09	[H + G EDV Vertriebs]	blacksuit	Link
2024-03-09	[Fincasrevuelta]	everest	Link
2024-03-09	[Lindsay Municipal Hospital]	bianlian	Link
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	Link
2024-03-09	[ACE Air Cargo]	hunters	Link
2024-03-09	[Watsonclinic.com]	donutleaks	Link
2024-03-06	[Continental Aerospace Technologies]	play	Link
2024-03-08	[redwoodcoastrc.org]	lockbit3	Link
2024-03-08	[PowerRail Distribution]	blacksuit	Link
2024-03-08	[Denninger's]	medusa	Link
2024-03-08	[SIEA]	ransomhub	Link
2024-03-08	[Hozzify]	ransomhub	Link
2024-03-07	[rmhfranchise.com]	lockbit3	Link
2024-03-07	[New York Home Healthcare]	bianlian	Link
2024-03-07	[Palmer Construction Co., Inc]	bianlian	Link
2024-03-07	[en-act-architecture]	qilin	Link
2024-03-07	[Merchant ID]	ransomhub	Link
2024-03-07	[SP Mundi]	ransomhub	Link
2024-03-07	[www.duvel.com]	stormous	Link
2024-03-06	[www.loghmanpharma.com]	stormous	Link
2024-03-06	[MainVest]	play	Link
2024-03-06	[C?????????? A???????e T???????????]	play	Link
2024-03-05	[Haivision MCS]	medusa	Link
2024-03-06	[Tocci Building Corporation]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-06	[JVCKENWOOD]	medusa	Link
2024-03-06	[American Renal Associates]	medusa	Link
2024-03-06	[US #1364 Federal Credit Union]	medusa	Link
2024-03-06	[viadirectamarketing]	stormous	Link
2024-03-06	[Liquid Environmental Solutions]	incransom	Link
2024-03-06	[Infosoft]	akira	Link
2024-03-06	[brightwires.com.sa]	qilin	Link
2024-03-06	[Medical Billing Specialists]	akira	Link
2024-03-06	[Telecentro]	akira	Link
2024-03-06	[Steiner (Austrian furniture makers)]	akira	Link
2024-03-06	[Biomedical Research Institute]	meow	Link
2024-03-06	[K???o???]	play	Link
2024-03-06	[Kudulis Reisinger Price]	8base	Link
2024-03-06	[Global Zone]	8base	Link
2024-03-06	[Mediplast AB]	8base	Link
2024-03-05	[airbogo]	stormous	Link
2024-03-05	[sunwave.com.cn]	lockbit3	Link
2024-03-05	[SJCME.EDU]	clop	Link
2024-03-05	[central.k12.or.us]	lockbit3	Link
2024-03-05	[iemsc.com]	qilin	Link
2024-03-05	[hawita-gruppe]	qilin	Link
2024-03-05	[Future Generations Foundation]	meow	Link
2024-03-04	[Seven Seas Group]	snatch	Link
2024-03-04	[Paul Davis Restoration]	medusa	Link
2024-03-04	[Veeco]	medusa	Link
2024-03-04	[dismogas]	stormous	Link
2024-03-04	[everplast]	stormous	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	Link
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link
2024-03-03	[valoremreply.com]	lockbit3	Link
2024-03-04	[Martin’s, Inc.]	bianlian	Link
2024-03-03	[Prompt Financial Solutions]	medusa	Link
2024-03-03	[Sophiahemmet University]	medusa	Link
2024-03-03	[Centennial Law Group LLP]	medusa	Link
2024-03-03	[Eastern Rio Blanco Metropolitan]	medusa	Link
2024-03-03	[Chris Argiropoulos Professional]	medusa	Link
2024-03-03	[THAISUMMIT.US]	clop	Link
2024-03-03	[THESAFIRCHOICE.COM]	clop	Link
2024-03-03	[ipmaltamira]	alphv	Link
2024-03-03	[earnesthealth.com]	lockbit3	Link
2024-03-03	[Ward Transport & Logistics]	dragonforce	Link
2024-03-03	[Ponoka.ca]	cloak	Link
2024-03-03	[stockdevelopment.com]	lockbit3	Link
2024-03-03	[Ewig Usa]	alphv	Link
2024-03-02	[aerospace.com]	lockbit3	Link
2024-03-02	[starkpower.de]	lockbit3	Link
2024-03-02	[roehr-stolberg.de]	lockbit3	Link
2024-03-02	[schuett-grundei.de]	lockbit3	Link
2024-03-02	[unitednotions.com]	lockbit3	Link
2024-03-02	[smuldes.com]	lockbit3	Link
2024-03-02	[esser-ps.de]	lockbit3	Link
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[Skyland Grain]	play	Link
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link
2024-03-01	[Powill Manufacturing & Engineering]	play	Link
2024-03-01	[Trans+Plus Systems]	play	Link
2024-03-01	[Hedlunds]	play	Link
2024-03-01	[Red River Title]	play	Link
2024-03-01	[Compact Mould]	play	Link
2024-03-01	[Winona Pattern & Mold]	play	Link
2024-03-01	[Marketon]	play	Link
2024-03-01	[Stack Infrastructure]	play	Link
2024-03-01	[Coastal Car]	play	Link
2024-03-01	[New Bedford Welding Supply]	play	Link
2024-03-01	[Influence Communication]	play	Link
2024-03-01	[Kool-air]	play	Link
2024-03-01	[FBi Construction]	play	Link
2024-03-01	[SBM & Co]	alphv	Link
2024-03-01	[Shooting House]	ransomhub	Link
2024-03-01	[Crystal Window & Door Systems]	dragonforce	Link
2024-03-01	[Gilmore Construction]	blacksuit	Link
2024-03-01	[Petrus Resources Ltd]	alphv	Link
2024-03-01	[CoreData]	akira	Link
2024-03-01	[Gansevoort Hotel Group]	akira	Link
2024-03-01	[DJI Company]	mogilevich	Link
2024-03-01	[Kick]	mogilevich	Link
2024-03-01	[Shein]	mogilevich	Link
2024-03-01	[Kumagai Gumi Group]	alphv	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.