Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240330

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

Neue SugarCRM-Versionen schließen kritische Lücken

Insgesamt 18, teils kritische Lücken schließen die neuen Versionen SugarCRM 13.03. und 12.05.

- Link

—

Google Chrome: Kritische Schwachstelle bedroht Browser-Nutzer

In Chrome haben Googles Entwickler sieben Sicherheitslücken abgedichtet. Mindestens eine davon stellt ein kritisches Risiko dar.

- Link

—

Loadbalancer: Sicherheitslücken in Loadmaster von Progress/Kemp

In der Loadbalancer-Software Loadmaster von Progress/Kemp klaffen Sicherheitslücken, durch die Angreifer etwa Befehle einschleusen können.

- Link

—

Sicherheitslücken in Microsofts WiX-Installer-Toolset gestopft

Das quelloffene WiX-Installer-Toolset von Microsoft hat zwei Sicherheitslücken. Die dichten aktualisierte Versionen ab.

- Link

—

Firefox: Notfall-Update schließt kritische Sicherheitslücken

Die Mozilla-Entwickler haben zwei kritische Sicherheitslücken mit dem Update auf Firefox 124.0.1 und Firefox ESR 115.9.1 geschlossen.

- Link

—

Kritische Sicherheitslücke in FortiClientEMS wird angegriffen

Eine kritische Schwachstelle in FortiClientEMS wird inzwischen aktiv angegriffen. Zudem ist ein Proof-of-Concept-Exploit öffentlich geworden.

- Link

—

Microsoft schließt Sicherheitslücke in Xbox-Gaming-Dienst – nach Hickhack

Microsoft hat ein Sicherheitsleck im Xbox Gaming Service abgedichtet. Dem ging jedoch eine Diskussion voraus.

- Link

—

IBM-Software: Angreifer können Systeme mit Schadcode kompromittieren

Es sind wichtige Sicherheitsupdates für IBM App Connect Enterprise und InfoSphere Information Server erschienen.

- Link

—

Lücken in Ruby-Gems ermöglichen Codeschmuggel und Datenleck

Angreifer könnten eigenen Code im Kontext eines Ruby-Programms ausführen. Nutzer der RDoc- und StringIO-Gems sollten aktualisierte Versionen einspielen.

- Link

—

Attacken auf Ivanti Standalone Sentry und Neurons möglich

Angreifer können an kritische Sicherheitslücken in Ivanti-Software ansetzen. Sicherheitsupdates sind 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	0.901600000	0.987320000	Link
CVE-2023-6553	0.916210000	0.988430000	Link
CVE-2023-5360	0.967230000	0.996390000	Link
CVE-2023-4966	0.964860000	0.995620000	Link
CVE-2023-47246	0.940270000	0.991030000	Link
CVE-2023-46805	0.964290000	0.995480000	Link
CVE-2023-46747	0.972020000	0.998070000	Link
CVE-2023-46604	0.973060000	0.998610000	Link
CVE-2023-43177	0.927670000	0.989710000	Link
CVE-2023-42793	0.970710000	0.997520000	Link
CVE-2023-39143	0.939910000	0.990970000	Link
CVE-2023-38646	0.916640000	0.988480000	Link
CVE-2023-38203	0.960070000	0.994410000	Link
CVE-2023-38035	0.972180000	0.998170000	Link
CVE-2023-36845	0.966640000	0.996210000	Link
CVE-2023-35813	0.905250000	0.987550000	Link
CVE-2023-3519	0.911860000	0.988130000	Link
CVE-2023-35082	0.932380000	0.990190000	Link
CVE-2023-35078	0.962290000	0.994880000	Link
CVE-2023-34960	0.935410000	0.990500000	Link
CVE-2023-34634	0.925600000	0.989450000	Link
CVE-2023-34362	0.962490000	0.994930000	Link
CVE-2023-34039	0.907130000	0.987740000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.904650000	0.987510000	Link
CVE-2023-33246	0.973410000	0.998830000	Link
CVE-2023-32315	0.973840000	0.999040000	Link
CVE-2023-32235	0.911650000	0.988100000	Link
CVE-2023-30625	0.948330000	0.992260000	Link
CVE-2023-30013	0.956040000	0.993600000	Link
CVE-2023-29300	0.962460000	0.994910000	Link
CVE-2023-29298	0.926460000	0.989540000	Link
CVE-2023-28771	0.917660000	0.988600000	Link
CVE-2023-28432	0.943220000	0.991430000	Link
CVE-2023-28121	0.938130000	0.990790000	Link
CVE-2023-27524	0.972270000	0.998230000	Link
CVE-2023-27372	0.971520000	0.997870000	Link
CVE-2023-27350	0.972040000	0.998090000	Link
CVE-2023-26469	0.943740000	0.991520000	Link
CVE-2023-26360	0.963570000	0.995250000	Link
CVE-2023-26035	0.969280000	0.997010000	Link
CVE-2023-25717	0.957880000	0.993940000	Link
CVE-2023-25194	0.968970000	0.996910000	Link
CVE-2023-2479	0.962540000	0.994940000	Link
CVE-2023-24489	0.973620000	0.998930000	Link
CVE-2023-23752	0.952140000	0.992890000	Link
CVE-2023-23397	0.923530000	0.989160000	Link
CVE-2023-23333	0.963260000	0.995160000	Link
CVE-2023-22527	0.965680000	0.995970000	Link
CVE-2023-22518	0.970110000	0.997270000	Link
CVE-2023-22515	0.971880000	0.998020000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.958450000	0.994040000	Link
CVE-2023-21554	0.959700000	0.994310000	Link
CVE-2023-20887	0.964080000	0.995420000	Link
CVE-2023-1671	0.961560000	0.994720000	Link
CVE-2023-0669	0.969540000	0.997100000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 28 Mar 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] SugarCRM Sugar Enterprise: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in SugarCRM Sugar Enterprise ausnutzen, um einen Cross Site Scripting oder einen SQL Injection Angriff durchzuführen, Daten zu manipulieren oder Code auszuführen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco IOS XE: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco IOS XE ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen, seine Privilegien zu erweitern oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco Aironet Access Point: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Cisco Aironet Access Point, Cisco Catalyst, Cisco Router und Cisco Small Business ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder

einen Denial of Service Zustand herbeizuführen.
- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco IOS: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco IOS und Cisco IOS XE ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Thu, 28 Mar 2024

[NEU] [UNGEPATCHT] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um Informationen offenzulegen oder um Sicherheitsmaßnahmen zu umgehen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] TLS: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in TLS 1.2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] python-cryptography: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in python-cryptography ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] dnsmasq: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in dnsmasq ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial of Service Angriff durchzuführen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

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

- Link

—

Thu, 28 Mar 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programm-

code auszuführen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Red Hat Advanced Cluster Management for Kubernetes: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Red Hat Advanced Cluster Management for Kubernetes ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Code auszuführen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.
- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM MQ ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/29/2024	[Linear eMerge Code RCE (CVE-2019-7256)]	critical
3/29/2024	[XZ Utils 5.6.0 / 5.6.1 SSH Backdoor (CVE-2024-3094)]	critical
3/28/2024	[Fedora 39 : csmock (2024-bd9e53683a)]	critical
3/28/2024	[Fedora 39 : ofono (2024-4e5613bcb3)]	critical
3/28/2024	[Fedora 38 : csmock (2024-816ffc9598)]	critical
3/28/2024	[Fedora 38 : ofono (2024-e8a02e129e)]	critical
3/30/2024	[Fedora 39 : cockpit (2024-6065341780)]	high
3/29/2024	[Slackware Linux 15.0 / current util-linux Vulnerability (SSA:2024-088-02)]	high
3/29/2024	[Slackware Linux 15.0 / current seamonkey Vulnerability (SSA:2024-088-01)]	high
3/29/2024	[Oracle Linux 8 : libreoffice (ELSA-2024-1514)]	high
3/29/2024	[Ubuntu 22.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6707-4)]	high
3/29/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6704-4)]	high
3/29/2024	[FreeBSD : Gitlab – vulnerabilities (d2992bc2-ed18-11ee-96dc-001b217b3468)]	high
3/29/2024	[Debian dsa-5648 : chromium - security update]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:1039-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 7 for SLE 15 SP5) (SUSE-SU-2024:1040-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 40 for SLE 15 SP3) (SUSE-SU-2024:1033-1)]	high
3/29/2024	[SUSE SLES12 Security Update : kernel (Live Patch 48 for SLE 12 SP5) (SUSE-SU-2024:1028-1)]	high
3/29/2024	[SUSE SLES15 Security Update : podman (SUSE-SU-2024:1059-1)]	high

Datum	Schwachstelle	Bewertung
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:1045-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP3) (SUSE-SU-2024:1054-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 31 for SLE 15 SP3) (SUSE-SU-2024:1047-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 43 for SLE 15 SP2) (SUSE-SU-2024:1053-1)]	high
3/29/2024	[SUSE SLES15 Security Update : podman (SUSE-SU-2024:1058-1)]	high
3/29/2024	[ForgeRock Access Management 7.2.0 / 7.1.x < 7.1.4 / 7.0.x <= 7.0.2 Path Traversal]	high
3/29/2024	[Security Updates for Microsoft Office Products C2R (March 2024)]	high
3/29/2024	[Atlassian Confluence < 7.19.20 / 7.20.x < 8.5.7 (CONFSERVER-94843)]	high
3/29/2024	[Curl 7.44.0 < 8.7.0 HTTP/2 Push Headers Memory-leak (CVE-2024-2398)]	high
3/29/2024	[Curl 8.6.0 < 8.7.0 QUIC Certificate Check Bypass (CVE-2024-2379)]	high
3/29/2024	[Curl 8.5.0 < 8.7.0 TLS Certificate Check Bypass (CVE-2024-2466)]	high
3/29/2024	[F5 Networks BIG-IP : DNS vulnerability (K000139092)]	high
3/28/2024	[SUSE SLES12 Security Update : MozillaFirefox (SUSE-SU-2024:1000-1)]	high
3/28/2024	[SUSE SLES15 Security Update : krb5 (SUSE-SU-2024:0999-1)]	high
3/28/2024	[Fedora 38 : chromium (2024-b4dab205d7)]	high
3/28/2024	[Fedora 39 : onnx (2024-270e3b5e9b)]	high
3/28/2024	[Fedora 39 : chromium (2024-0bb0e8f2a0)]	high

Datum	Schwachstelle	Bewertung
3/28/2024	[Fedora 39 : emacs (2024-de10068888)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 29 Mar 2024

WatchGuard XTM Firebox Unauthenticated Remote Command Execution

This Metasploit module exploits a buffer overflow at the administration interface (8080 or 4117) of WatchGuard Firebox and XTM appliances which is built from a cherrypy python backend sending XML-RPC requests to a C binary called wgagent using pre-authentication endpoint /agent/login. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. Successful exploitation results in remote code execution as user nobody.

- Link

—

” “Fri, 29 Mar 2024

Soholaunch 4.9.4 r44 Shell Upload

Soholaunch version 4.9.4 r44 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Local File Inclusion

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a local file inclusion vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Server-Side Template Injection

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a server-side template injection vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Command Injection

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a command injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Event Management 1.0 SQL Injection

Event Management version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

util-linux wall Escape Sequence Injection

The util-linux wall command does not filter escape sequences from command line arguments. The vulnerable code was introduced in commit cdd3cc7fa4 (2013). Every version since has been vulnerable. This allows unprivileged users to put arbitrary text on other users terminals, if mesg is set to y and wall is setgid. CentOS is not vulnerable since wall is not setgid. On Ubuntu 22.04 and Debian Bookworm, wall is both setgid and mesg is set to y by default.

- Link

—

” “Thu, 28 Mar 2024

Circontrol Raption Buffer Overflow / Command Injection

The server in Circontrol Raption versions through 5.11.2 has a pre-authentication stack-based buffer overflow that can be exploited to gain run-time control of the device as root. The pwrstudio web application of EV Charger (in the server in Circontrol Raption through 5.6.2) is vulnerable to OS command injection.

- Link

—

” “Thu, 28 Mar 2024

FusionPBX Session Fixation

FusionPBX suffers from a session fixation vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Dell Security Management Server Privilege Escalation

Dell Security Management Server versions prior to 11.9.0 suffer from a local privilege escalation vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Purei CMS 1.0 SQL Injection

Purei CMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Workout Journal App 1.0 Cross Site Scripting

Workout Journal App version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 28 Mar 2024

LMS PHP 1.0 SQL Injection

LMS PHP version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Asterisk AMI 18.20.0 File Content / Path Disclosure

Asterisk AMI version 18.20.0 suffers from authenticated partial file content and path disclosure vulnerabilities.

- Link

—

” “Thu, 28 Mar 2024

Siklu MultiHaul TG Series Credential Disclosure

Siklu MultiHaul TG Series versions prior to 2.0.0 suffer from an unauthenticated credential disclosure vulnerability.

- Link

—

” “Thu, 28 Mar 2024

RouterOS 6.44 / 6.49.10 Denial Of Service

RouterOS versions 6.40.5 through 6.44 and 6.48.1 through 6.49.10 suffers from a denial of service vulnerability.

- Link

—

” “Thu, 28 Mar 2024

NodeBB 3.6.7 Broken Access Control

NodeBB version 3.6.7 suffers from a broken access control that lets attackers via data only meant for an administrator.

- Link

—

” “Thu, 28 Mar 2024

WinRAR 6.22 Remote Code Execution

WinRAR version 6.22 suffers from a remote code execution vulnerability via a malicious zip archive.
- Link

—

” “Wed, 27 Mar 2024

Sharepoint Dynamic Proxy Generator Remote Command Execution

This Metasploit module exploits two vulnerabilities in Sharepoint 2019 - an authentication bypass as noted in CVE-2023-29357 which was patched in June of 2023 and CVE-2023-24955 which was a remote command execution vulnerability patched in May of 2023. The authentication bypass allows attackers to impersonate the Sharepoint Admin user. This vulnerability stems from the signature validation check used to verify JSON Web Tokens (JWTs) used for OAuth authentication. If the signing algorithm of the user-provided JWT is set to none, SharePoint skips the signature validation step due to a logic flaw in the ReadTokenCore() method. After impersonating the administrator user, the attacker has access to the Sharepoint API and is able to exploit CVE-2023-24955. This authenticated remote command execution vulnerability leverages the impersonated privileged account to replace the /BusinessDataMetadataCatalog/BDCMetadata.bdcm file in the webroot directory with a payload. The payload is then compiled and executed by Sharepoint allowing attackers to remotely execute commands via the API.
- Link

—

” “Wed, 27 Mar 2024

WordPress Bricks Builder Theme 1.9.6 Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in the Bricks Builder Theme versions 1.9.6 and below for WordPress. The vulnerability allows attackers to execute arbitrary PHP code by leveraging a nonce leakage to bypass authentication and exploit the eval() function usage within the theme. Successful exploitation allows for full control of the affected WordPress site. It is recommended to upgrade to version 1.9.6.1 or higher.
- Link

—

” “Wed, 27 Mar 2024

Artica Proxy Unauthenticated PHP Deserialization

A command injection vulnerability in Artica Proxy appliance versions 4.50 and 4.40 allows remote attackers to run arbitrary commands via an unauthenticated HTTP request. The Artica Proxy administrative web application will deserialize arbitrary PHP objects supplied by unauthenticated users and subsequently enable code execution as the www-data user.
- Link

—

” “Tue, 26 Mar 2024

Bludit 3.13.0 Cross Site Scripting

Bludit version 3.13.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 26 Mar 2024
Insurance Management System PHP And MySQL 1.0 Cross Site Scripting
Insurance Management System PHP and MySQL version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Tue, 26 Mar 2024
Craft CMS 4.4.14 Remote Code Execution
Craft CMS version 4.4.14 suffers from an unauthenticated remote code execution vulnerability.
- Link
—
” “Tue, 26 Mar 2024
LimeSurvey Community 5.3.32 Cross Site Scripting
LimeSurvey Community version 5.3.32 suffers from a persistent cross site scripting vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Thu, 28 Mar 2024
ZDI-24-356: Siemens Simcenter Femap MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Thu, 28 Mar 2024
ZDI-24-355: Wireshark NetScreen File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Thu, 28 Mar 2024
ZDI-24-354: Schneider Electric EcoStruxure Power Design - Ecodial BinSerializer Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—

” “Thu, 28 Mar 2024

ZDI-24-353: Softing edgeConnector Siemens Cleartext Transmission of Credentials Authentication Bypass Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-352: Softing edgeConnector Siemens Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-351: SolarWinds Access Rights Manager OpenFileStreamLocal Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-350: SolarWinds Access Rights Manager JsonSerializationHelper Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-349: SolarWinds Access Rights Manager OpenFile Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-348: SolarWinds Access Rights Manager openServerFileStream Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-347: SolarWinds Access Rights Manager JsonSerializationBinder Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-346: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-345: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-344: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-343: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-342: Foxit PDF Reader U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-341: Foxit PDF Reader U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-340: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-339: Foxit PDF Reader PDF File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-338: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-337: Foxit PDF Reader AcroForm Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-336: Foxit PDF Reader AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-335: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-334: Foxit PDF Reader AcroForm Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-333: Foxit PDF Reader Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-332: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-331: Foxit PDF Reader AcroForm Annotation Type Confusion Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-330: Foxit PDF Reader AcroForm User-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-329: Foxit PDF Reader AcroForm 3D Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-328: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-327: Foxit PDF Reader U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-326: Foxit PDF Reader U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-325: Foxit PDF Reader U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-324: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-323: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-322: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-321: Foxit PDF Reader Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-320: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-319: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-318: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-317: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-316: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-315: Foxit PDF Reader Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-314: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-313: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-312: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-311: Foxit PDF Reader template Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-310: Foxit PDF Reader Annotation Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-309: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-308: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-307: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-306: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-305: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-304: Foxit PDF Reader AcroForm Annotation Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-303: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-302: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-301: Foxit PDF Reader template Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-300: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-299: Linux Kernel nft_exthdr_ipv6_eval Stack-based Buffer Overflow Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-298: Linux Kernel nft_exthdr_tcp_eval Stack-based Buffer Overflow Information Disclosure Vulnerability

- Link

—

” “Thu, 28 Mar 2024

ZDI-24-297: Linux Kernel nft_exthdr_sctp_eval Stack-based Buffer Overflow Information Disclosure Vulnerability

- Link

—

” “Wed, 27 Mar 2024

ZDI-24-296: Autodesk DWG TrueView DWG File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 27 Mar 2024

ZDI-24-295: Autodesk FBX Review ABC File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

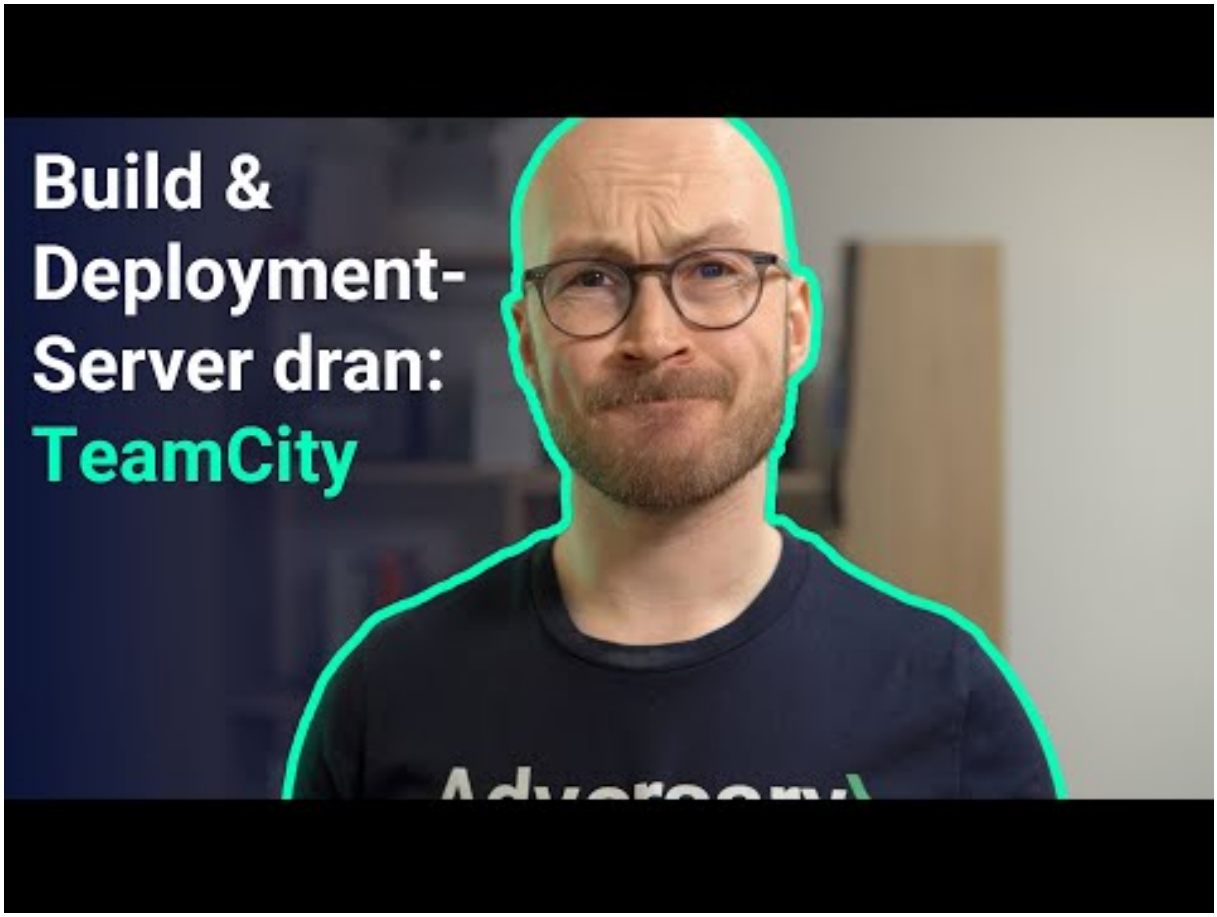
—

”

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
2024-03-26	Gilmer County	[USA]	Link
2024-03-26	Unimed VTRP	[BRA]	Link
2024-03-25	City of St. Cloud	[USA]	Link
2024-03-24	Ariza Credit Union	[GRD]	Link
2024-03-24	VNDirect	[VNM]	Link
2024-03-24	Intermarché by Mestdagh	[BEL]	Link
2024-03-24	Université de Winnipeg	[CAN]	Link
2024-03-22	Cressex Community School	[GBR]	Link
2024-03-21	Tarrant Appraisal District	[USA]	Link
2024-03-20	Nampak	[ZAF]	Link
2024-03-19	Goed	[BEL]	Link
2024-03-18	Unimed Cuiabá	[BRA]	Link
2024-03-18	Comté de Henry, Illinois	[USA]	Link
2024-03-17	Ville de Pensacola	[USA]	Link
2024-03-17	South China Athletic Association	[HKG]	Link
2024-03-17	Polycab	[IND]	Link
2024-03-15	Fujitsu	[JPN]	Link
2024-03-15	Deutsches Meeresmuseum de Stralsund	[DEU]	Link
2024-03-15	Communauté de communes de Nuits-Saint-Georges	[FRA]	Link
2024-03-15	Trifyl	[FRA]	Link
2024-03-14	NHS Dumfries and Galloway	[GBR]	Link
2024-03-14	Scranton School District	[USA]	Link
2024-03-14	Radiant Logistics, Inc.	[USA]	Link
2024-03-13	Maxis	[MYS]	Link
2024-03-12	Riverview School District	[USA]	Link

Datum	Opfer	Land	Information
2024-03-11	District de North Vancouver	[CAN]	Link
2024-03-11	Scullion Law	[GBR]	Link
2024-03-10	edpnet	[BEL]	Link
2024-03-10	Town of Huntsville	[CAN]	Link
2024-03-10	MarineMax	[USA]	Link
2024-03-10	EDIS	[AUT]	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
2024-03-07	Opheor	[FRA]	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
2024-03-29	[W?????? ????????y]	play	Link
2024-03-29	[Control Technology]	akira	Link
2024-03-29	[Graypen Ltd]	incransom	Link
2024-03-29	[Sysmex]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-29	[rameywine.com]	abyss	Link
2024-03-29	[Lodan Electronics Inc]	incransom	Link
2024-03-29	[PSEC Church]	incransom	Link
2024-03-29	[Tech-Quip Inc]	incransom	Link
2024-03-05	[K2systems.ca]	redransomware	Link
2024-03-05	[Sfi-wfc.com]	redransomware	Link
2024-03-05	[Bendallmednick]	redransomware	Link
2024-03-05	[Comohotels.com]	redransomware	Link
2024-03-05	[Aluminumtrailer.com]	redransomware	Link
2024-03-05	[Southcoindustries.com]	redransomware	Link
2024-03-05	[Kogok.com]	redransomware	Link
2024-03-05	[Baystate.edu]	redransomware	Link
2024-03-05	[Tecnolite.com]	redransomware	Link
2024-03-05	[Solucionesls.com]	redransomware	Link
2024-03-05	[Saglobal.com]	redransomware	Link
2024-03-05	[Thors-Data.dk]	redransomware	Link
2024-03-28	[Avant IT Norway]	ransomhub	Link
2024-03-28	[Lakes Precision]	akira	Link
2024-03-28	[Neurobehavioral Medicine Consultants]	bianlian	Link
2024-03-28	[Santa Cruz Seaside]	akira	Link
2024-03-28	[Florida Memorial University]	incransom	Link
2024-03-28	[Reeves-Wiedeman]	bianlian	Link
2024-03-28	[Exela Technologies]	hunters	Link
2024-03-28	[Primeimaging Data Leak]	everest	Link
2024-03-27	[Otolaryngology Associates]	incransom	Link
2024-03-27	[anovahealth.com]	lockbit3	Link
2024-03-27	[PT Bank Pembangunan Daerah Banten Tbk]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-27	[vilis.com]	blackbasta	Link
2024-03-27	[pstrans.com]	blackbasta	Link
2024-03-27	[fpdcompany.com]	blackbasta	Link
2024-03-27	[northamericansigns.com]	blackbasta	Link
2024-03-27	[otrwheel.com]	blackbasta	Link
2024-03-27	[prodrive.com]	blackbasta	Link
2024-03-27	[dgse.com]	blackbasta	Link
2024-03-27	[Summer Fresh]	qilin	Link
2024-03-27	[Pavilion Construction]	play	Link
2024-03-27	[Boingo Graphics]	play	Link
2024-03-27	[bulwarkpestcontrol.com]	blackbasta	Link
2024-03-27	[lagunitas.com]	blackbasta	Link
2024-03-27	[carolinafoodsinc.com]	blackbasta	Link
2024-03-27	[ero-etikett.com]	blackbasta	Link
2024-03-27	[amerlux.com]	blackbasta	Link
2024-03-27	[organizedliving.com]	blackbasta	Link
2024-03-27	[mjcelco.com]	blackbasta	Link
2024-03-27	[kmbdg.com]	blackbasta	Link
2024-03-27	[pctinternational.com]	blackbasta	Link
2024-03-27	[theshootingwarehouse.com]	blackbasta	Link
2024-03-27	[Mermet]	akira	Link
2024-03-27	[Tbr Kowalczyk]	play	Link
2024-03-27	[JM Thompson]	play	Link
2024-03-27	[Weld Plus]	play	Link
2024-03-27	[qosina.com]	cactus	Link
2024-03-27	[Festspielhaus Baden-Baden]	play	Link
2024-03-27	[West Monroe]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-27	[Frawner]	play	Link
2024-03-27	[Alber Law Group]	play	Link
2024-03-27	[Hartz]	play	Link
2024-03-27	[Quality Enclosures]	play	Link
2024-03-27	[Lawrence Semiconductor Research Laboratory]	play	Link
2024-03-27	[Lambda Energy Resources]	play	Link
2024-03-27	[dkpvlaw.com]	lockbit3	Link
2024-03-27	[lifelinedatacenters.com]	lockbit3	Link
2024-03-27	[countryvillahealthservices.com]	lockbit3	Link
2024-03-27	[lindquistinsurance.com]	abyss	Link
2024-03-27	[pcscivilinc.com]	lockbit3	Link
2024-03-27	[krueth.de]	lockbit3	Link
2024-03-26	[NHS Scotland]	incransom	Link
2024-03-27	[tmt-mc.jp]	lockbit3	Link
2024-03-27	[contenderboats.com]	cactus	Link
2024-03-27	[HC Querétaro]	8base	Link
2024-03-27	[UNDP]	8base	Link
2024-03-27	[Lindos Group Of Companies]	8base	Link
2024-03-27	[isophon glas GmbH]	8base	Link
2024-03-26	[Miki Travel Limited]	snatch	Link
2024-03-26	[nampak.com]	lockbit3	Link
2024-03-26	[El Debate]	rhysida	Link
2024-03-26	[SummerFresh]	qilin	Link
2024-03-26	[polycab.com]	lockbit3	Link
2024-03-26	[Barrie and Community Family Health Team]	incransom	Link
2024-03-26	[Lieberman LLP]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-26	[Affiliated Dermatologists and Dermatologic Surgeons]	bianlian	Link
2024-03-26	[Koi Design]	akira	Link
2024-03-26	[Tanis Brush]	akira	Link
2024-03-26	[Crimsgroup]	everest	Link
2024-03-26	[Woodsboro ISD]	ransomhub	Link
2024-03-25	[regencymedia.com.au]	lockbit3	Link
2024-03-25	[wblight.com]	lockbit3	Link
2024-03-25	[CLARK Material Handling Company]	hunters	Link
2024-03-25	[Dunbier Boat Trailers]	dragonforce	Link
2024-03-25	[Big Issue Group]	qilin	Link
2024-03-25	[Greenline Service]	dragonforce	Link
2024-03-25	[Teton Orthopaedics]	dragonforce	Link
2024-03-25	[Calida]	akira	Link
2024-03-25	[Vita IT]	akira	Link
2024-03-25	[European Centre for Compensation]	akira	Link
2024-03-25	[Burnham Wood Charter Schools]	qilin	Link
2024-03-25	[kh.org]	threeam	Link
2024-03-25	[Ejército del Per]	incransom	Link
2024-03-25	[Law Offices of John V. Orrick, P.L.]	incransom	Link
2024-03-25	[Pantana CPA]	incransom	Link
2024-03-19	[Hallesche Kraftverkehrs & Speditions GmbH]	hunters	Link
2024-03-24	[Vhs-vaterstetten.de]	cloak	Link
2024-03-24	[Gascontec.com]	cloak	Link
2024-03-24	[Equatorial Energia]	cloak	Link
2024-03-23	[SchwarzGrantz]	raworld	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-23	[Title Management Inc]	raworld	Link
2024-03-23	[Pascoe International]	raworld	Link
2024-03-23	[Regina Dental Group]	medusa	Link
2024-03-23	[Impac Mortgage Holdings]	medusa	Link
2024-03-22	[Power Generation Engineering and Services Company (PGESCo) - pgesco.com]	ransomhub	Link
2024-03-22	[Bira 91]	bianlian	Link
2024-03-22	[Chambers Construction Co.]	bianlian	Link
2024-03-22	[newagesys.com]	cactus	Link
2024-03-22	[kelson.on.ca]	cactus	Link
2024-03-22	[flynncompanies.com]	blackbasta	Link
2024-03-22	[Casa Santiveri]	qilin	Link
2024-03-21	[ptsmi.co.id]	qilin	Link
2024-03-21	[Industrial de Alimentos EYL SA]	ransomhub	Link
2024-03-21	[politiaromana.ro]	killsec	Link
2024-03-21	[rabitbd.com]	killsec	Link
2024-03-21	[pbgbank.com]	killsec	Link
2024-03-21	[excellifecoaching.com]	killsec	Link
2024-03-21	[keralapolice.gov.in]	killsec	Link
2024-03-21	[Henry County, Illinois]	medusa	Link
2024-03-21	[northerncasket.com]	lockbit3	Link
2024-03-21	[tmbs.ch]	lockbit3	Link
2024-03-21	[pathologie-bochum.de]	lockbit3	Link
2024-03-21	[La Pastina]	ransomhub	Link
2024-03-21	[Bisco Industries]	raworld	Link
2024-03-21	[Bluelinea]	raworld	Link
2024-03-21	[Deepnoid]	raworld	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-21	[Eastern Media International Corporation]	raworld	Link
2024-03-21	[Eyegene]	raworld	Link
2024-03-21	[Insurance Providers Group]	raworld	Link
2024-03-21	[Thaire]	raworld	Link
2024-03-21	[Decimal Point Analytics Pvt]	raworld	Link
2024-03-21	[Wealth Enhancement Group]	raworld	Link
2024-03-21	[Zurvita]	raworld	Link
2024-03-21	[Piex Group]	raworld	Link
2024-03-21	[Yuxin Automobile Co.Ltd]	raworld	Link
2024-03-21	[24/7 Express Logistics]	raworld	Link
2024-03-21	[Aceromex]	raworld	Link
2024-03-21	[Chung Hwa Chemical Industrial Works]	raworld	Link
2024-03-21	[SUMMIT VETERINARY PHARMACEUTICALS LIMITED]	raworld	Link
2024-03-21	[Informist Media]	raworld	Link
2024-03-21	[ALAB laboratoria]	raworld	Link
2024-03-21	[Di Martino Group]	raworld	Link
2024-03-21	[Rockford Gastroenterology Associates]	raworld	Link
2024-03-21	[HALLIDAYS GROUP LIMITED]	raworld	Link
2024-03-21	[Die Unfallkasse Thüringen]	raworld	Link
2024-03-21	[NIDEC GPM GmbH]	raworld	Link
2024-03-21	[Wurzbacher]	raworld	Link
2024-03-21	[Ranzijn]	raworld	Link
2024-03-21	[SHORTERM GROUP]	raworld	Link
2024-03-20	[MarineMax]	rhysida	Link
2024-03-20	[Suburban Surgical Care Specialists]	medusa	Link
2024-03-20	[igf-inc.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-20	[logistasolutions.com]	blackbasta	Link
2024-03-20	[oceaneering.com]	blackbasta	Link
2024-03-20	[interluxury.com]	blackbasta	Link
2024-03-20	[Kolbe Striping]	rhysida	Link
2024-03-20	[Springfield Sign]	8base	Link
2024-03-20	[ÖSTENSSONS LIVS AB]	8base	Link
2024-03-20	[Filexis AG Treuhand und Immobilien]	8base	Link
2024-03-20	[South Star Electronics]	trigona	Link
2024-03-19	[Accipiter Capital Management, LLC]	medusa	Link
2024-03-19	[Urban Strategies]	medusa	Link
2024-03-19	[Sting AD]	hunters	Link
2024-03-19	[Jasper-Dubois County Public Library]	dragonforce	Link
2024-03-19	[Therapeutic Health Services]	hunters	Link
2024-03-19	[Panzeri Cattaneo]	hunters	Link
2024-03-19	[Retirement Line]	snatch	Link
2024-03-19	[Delta Pipeline]	bianlian	Link
2024-03-19	[Mayer Antonellis Jachowicz & Haranas, LLP]	bianlian	Link
2024-03-19	[P&B Capital Group]	bianlian	Link
2024-03-17	[Butler, Lavanceau & Sober]	snatch	Link
2024-03-18	[Dr. Leeman ENT]	bianlian	Link
2024-03-18	[HSI]	hunters	Link
2024-03-18	[AGL]	hunters	Link
2024-03-18	[Sun Holdings]	hunters	Link
2024-03-17	[paginesi]	stormous	Link
2024-03-18	[eclinicalsol.com]	cactus	Link
2024-03-18	[grupatopex.com]	cactus	Link
2024-03-18	[activeconceptsllc.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-17	[Romark Laboratories]	medusa	Link
2024-03-18	[crinetics.com]	lockbit3	Link
2024-03-03	[highfashion.com.hk]	mallox	Link
2024-03-14	[Ramdev Chemical Industries]	mallox	Link
2024-03-16	[Rafum Group]	mallox	Link
2024-03-16	[Autorità di Sistema Portuale del Mar Tirreno Settentrionale It]	medusa	Link
2024-03-16	[Elior UK]	medusa	Link
2024-03-16	[Indoarsip]	trigona	Link
2024-03-16	[Bwizer]	trigona	Link
2024-03-16	[Topa Partners]	trigona	Link
2024-03-16	[HUDSONBUSSALES.COM]	clop	Link
2024-03-15	[Desco Steel]	medusa	Link
2024-03-15	[Metzger Veterinary Services]	medusa	Link
2024-03-16	[Consolidated Benefits Resources]	bianlian	Link
2024-03-16	[agribank.com.na]	lockbit3	Link
2024-03-16	[triella.com]	lockbit3	Link
2024-03-16	[rrib.com]	lockbit3	Link
2024-03-16	[newmans-online.co.uk]	lockbit3	Link
2024-03-16	[hdstrading.com]	lockbit3	Link
2024-03-16	[duttonbrock.com]	lockbit3	Link
2024-03-16	[colefabrics.com]	lockbit3	Link
2024-03-16	[bergmeister.eu]	lockbit3	Link
2024-03-16	[automotionshade.com]	lockbit3	Link
2024-03-16	[Miki Travel]	hunters	Link
2024-03-16	[certifiedcollection.com]	lockbit3	Link
2024-03-16	[Acculabs Inc]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-08	[oyaksgs.com.tr]	lockbit3	Link
2024-03-15	[elezabypharmacy.com]	lockbit3	Link
2024-03-15	[South St Paul Public Schools]	blacksuit	Link
2024-03-12	[ATL Leasing]	hunters	Link
2024-03-14	[lostlb]	stormous	Link
2024-03-14	[education.eeb-lost]	stormous	Link
2024-03-14	[worthenind.com]	lockbit3	Link
2024-03-14	[rushenergyservices.com]	lockbit3	Link
2024-03-14	[sbmandco.com]	lockbit3	Link
2024-03-14	[mckimcreed.com]	lockbit3	Link
2024-03-14	[moperry.com]	lockbit3	Link
2024-03-14	[Cosmocolor]	hunters	Link
2024-03-14	[voidinteractive.net you are welcome in our chat]	donutleaks	Link
2024-03-14	[journeyfreight.com]	lockbit3	Link
2024-03-14	[dhanisisd.net]	lockbit3	Link
2024-03-14	[mioa.gov]	stormous	Link
2024-03-14	[gfad.de]	blackbasta	Link
2024-03-14	[Keboda Technology Co., Ltd.]	bianlian	Link
2024-03-14	[iamdesign.com]	abyss	Link
2024-03-14	[yarco.com]	abyss	Link
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.