
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240222



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	10
4 Aktiv ausgenutzte Sicherheitslücken	12
4.1 Exploits der letzten 5 Tage	12
4.2 0-Days der letzten 5 Tage	17
5 Die Hacks der Woche	19
5.0.1 Zahnbürsten DDoS und bald hat Ivanti die OWASP Top 10 voll...	19
6 Cyberangriffe: (Feb)	20
7 Ransomware-Erpressungen: (Feb)	21
8 Quellen	32
8.1 Quellenverzeichnis	32
9 Impressum	33

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

Broadcom schließt Sicherheitslücken in VMware Aria Operations und EAP-Plug-in

Broadcom verteilt Updates für VMware Aria Operations und das EAP Browser Plug-in. Sie bessern teils kritische Sicherheitslücken aus.

- [Link](#)

—

Firefox und Thunderbird: Neue Versionen liefern Sicherheitsfixes

Neue Versionen von Firefox, Firefox ESR und Thunderbird stehen bereit. Sie dichten im Kern Sicherheitslücken ab.

- [Link](#)

—

Google Chrome 122: Zwölf Sicherheitslecks gestopft

Der Versionszweig 122 von Google Chrome bessert vor allem zwölf Schwachstellen aus.

- [Link](#)

—

Jetzt updaten: Kritische Codeschmuggel-Lücken in Connectwise Screenconnect

In der Remote-Desktop-Software Screenconnect von Connectwise klaffen teils kritische Sicherheitslücken. Sie erlauben das Einschleusen von Schadcode.

- [Link](#)

—

Solarwinds: Codeschmuggel möglich, Updates verfügbar

Solarwinds schließt Sicherheitslücken in Access Rights Manager und Platform (Orion). Angreifer können Schadcode einschleusen.

- [Link](#)

—

Eset: Schwachstelle in Hintergrundscanner löscht beliebige Dateien

Der Hintergrundwächter der Eset-Virens Scanner enthält eine Schwachstelle, durch die bösartige Akteure Dateien mit Systemrechten löschen können.

- [Link](#)

—

Node.js: Sicherheitsupdates beheben Codeschmuggel und Serverabstürze

Neben Problemen im Kern des Projekts aktualisiert das Node-Projekt auch einige externe Bibliotheken.

- [Link](#)

—

Jetzt patchen! Angreifer nutzen kritische Lücke in Microsoft Exchange Server aus

Derzeit verschaffen sich Angreifer Zugriffe auf Exchange Server, um diese zu kompromittieren. Schutzlösungen sind verfügbar.

- [Link](#)

—

AMD meldet zahlreiche Sicherheitslücken in Prozessoren

AMD hat Sicherheitsmitteilungen zu Schwachstellen in diversen Prozessoren veröffentlicht. Firmwareupdates sollen sie ausbessern.

- [Link](#)

—

Webkonferenz-Tool Zoom: Rechteausweitung durch kritische Schwachstelle

Zoom warnt vor mehreren Schwachstellen in den Produkten des Unternehmens. Eine gilt als kritisches Sicherheitsrisiko.

- [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-2023-6553	0.916210000	0.988160000	Link
CVE-2023-5360	0.967230000	0.996300000	Link
CVE-2023-4966	0.963970000	0.995200000	Link
CVE-2023-47246	0.943540000	0.991270000	Link
CVE-2023-46805	0.962740000	0.994820000	Link
CVE-2023-46747	0.971390000	0.997740000	Link
CVE-2023-46604	0.972850000	0.998430000	Link
CVE-2023-43177	0.932620000	0.989970000	Link
CVE-2023-42793	0.973130000	0.998600000	Link
CVE-2023-41265	0.915100000	0.988030000	Link
CVE-2023-39143	0.925430000	0.989160000	Link
CVE-2023-38646	0.903940000	0.987110000	Link
CVE-2023-38205	0.932790000	0.990000000	Link
CVE-2023-38035	0.974110000	0.999230000	Link
CVE-2023-36845	0.964780000	0.995420000	Link
CVE-2023-3519	0.912410000	0.987850000	Link
CVE-2023-35082	0.962890000	0.994880000	Link
CVE-2023-35078	0.949930000	0.992260000	Link
CVE-2023-34960	0.931300000	0.989800000	Link
CVE-2023-34634	0.919000000	0.988460000	Link
CVE-2023-34362	0.959040000	0.993950000	Link
CVE-2023-3368	0.928930000	0.989490000	Link
CVE-2023-33246	0.973410000	0.998770000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32315	0.973860000	0.999030000	Link
CVE-2023-32235	0.902020000	0.987000000	Link
CVE-2023-30625	0.951530000	0.992520000	Link
CVE-2023-30013	0.936180000	0.990290000	Link
CVE-2023-29300	0.959640000	0.994100000	Link
CVE-2023-28771	0.923800000	0.989000000	Link
CVE-2023-28121	0.933120000	0.990030000	Link
CVE-2023-27524	0.972330000	0.998200000	Link
CVE-2023-27372	0.970420000	0.997330000	Link
CVE-2023-27350	0.972270000	0.998170000	Link
CVE-2023-26469	0.936750000	0.990380000	Link
CVE-2023-26360	0.960730000	0.994380000	Link
CVE-2023-26035	0.969370000	0.996950000	Link
CVE-2023-25717	0.962180000	0.994670000	Link
CVE-2023-2479	0.964780000	0.995420000	Link
CVE-2023-24489	0.973500000	0.998830000	Link
CVE-2023-23752	0.949820000	0.992240000	Link
CVE-2023-23397	0.904540000	0.987130000	Link
CVE-2023-22527	0.964800000	0.995430000	Link
CVE-2023-22518	0.969180000	0.996880000	Link
CVE-2023-22515	0.973330000	0.998730000	Link
CVE-2023-21839	0.962110000	0.994650000	Link
CVE-2023-21554	0.961220000	0.994450000	Link
CVE-2023-20887	0.965640000	0.995790000	Link
CVE-2023-20198	0.919220000	0.988480000	Link
CVE-2023-1671	0.964220000	0.995270000	Link
CVE-2023-0669	0.968020000	0.996560000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 21 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[NEU] [hoch] HP LaserJet: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in HP LaserJet ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[NEU] [hoch] Liferay Portal und Liferay DXP: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Liferay Portal und Liferay DXP ausnutzen, um einen Cross-Site Scripting Angriff zu starten, vertrauliche Informationen offenzulegen oder Dateien zu manipulieren.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder unbekannte Auswirkungen zu verursachen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Apache Struts: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Struts ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Wed, 21 Feb 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente "python-reportlab" ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Jenkins Plugins: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Jenkins Plugins ausnutzen, um einen CSRF-Angriff durchzuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder Dateien zu manipulieren.

- [Link](#)

—

Wed, 21 Feb 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, 21 Feb 2024

[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](#)

—

Wed, 21 Feb 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, 21 Feb 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (Pillow): Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] CUPS: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS, Debian Linux und SUSE Linux ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 21 Feb 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 21 Feb 2024

[UPDATE] [hoch] Android Patchday August 2022

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/22/2024	[Fedora 38 : rust-asyncgit / rust-bat / rust-cargo-c / rust-eza / etc (2024-993d3a78dd)]	critical
2/21/2024	[SUSE SLED12 / SLES12 Security Update : webkit2gtk3 (SUSE-SU-2024:0545-1)]	critical
2/21/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2024:0548-1)]	critical
2/21/2024	[Ubuntu 16.04 LTS : Libspfp2 vulnerabilities (USN-6584-2)]	critical
2/21/2024	[Debian dsa-5627 : firefox-esr - security update]	critical

Datum	Schwachstelle	Bewertung
2/21/2024	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2024-052-01)]	critical
2/21/2024	[Fedora 38 : freeglut (2024-0356803680)]	high
2/21/2024	[RHEL 8 : kernel (RHSA-2024:0930)]	high
2/21/2024	[SUSE SLES12 Security Update : libxml2 (SUSE-SU-2024:0556-1)]	high
2/21/2024	[SUSE SLES12 Security Update : dpdk (SUSE-SU-2024:0554-1)]	high
2/21/2024	[SUSE SLES15 / openSUSE 15 Security Update : openvswitch (SUSE-SU-2024:0553-1)]	high
2/21/2024	[SUSE SLES12 Security Update : libssh (SUSE-SU-2024:0539-1)]	high
2/21/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql16 (SUSE-SU-2024:0550-1)]	high
2/21/2024	[SUSE SLES12 Security Update : openvswitch (SUSE-SU-2024:0544-1)]	high
2/21/2024	[SUSE SLES12 Security Update : postgresql12 (SUSE-SU-2024:0542-1)]	high
2/21/2024	[SUSE SLES12 Security Update : postgresql13 (SUSE-SU-2024:0541-1)]	high
2/21/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2024:0551-1)]	high
2/21/2024	[SUSE SLES12 Security Update : postgresql16 (SUSE-SU-2024:0546-1)]	high
2/21/2024	[SUSE SLES12 Security Update : postgresql14 (SUSE-SU-2024:0540-1)]	high
2/21/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql14 (SUSE-SU-2024:0552-1)]	high
2/21/2024	[SUSE SLES15 / openSUSE 15 Security Update : hdf5 (SUSE-SU-2024:0538-1)]	high

Datum	Schwachstelle	Bewertung
2/21/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libxml2 (SUSE-SU-2024:0555-1)]	high
2/21/2024	[CentOS 8 : sudo (CESA-2024:0811)]	high
2/21/2024	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.2010)]	high
2/21/2024	[Debian dla-3736 : libunbound-dev - security update]	high
2/21/2024	[Oracle Linux 8 : .NET / 8.0 (ELSA-2024-0827)]	high
2/21/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6647-1)]	high
2/21/2024	[Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).]	high
2/21/2024	[Oracle Linux 8 : gimp:2.8 (ELSA-2024-0861)]	high
2/21/2024	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.7.1.6)]	high
2/21/2024	[GLSA-202402-29 : LibreOffice: Multiple Vulnerabilities]	high
2/21/2024	[GitLab 16.9 < 16.9.1 (CVE-2024-1451)]	high
2/21/2024	[RHEL 8 : Red Hat Virtualization (RHSA-2024:0934)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 21 Feb 2024

OpenOLAT 18.1.5 Cross Site Scripting / Privilege Escalation

OpenOLAT versions 18.1.4 and below and versions 18.1.5 and below suffer from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Wed, 21 Feb 2024

Yealink Configuration Encrypt Tool Static AES Key

A single, vendorwide, hardcoded AES key in the Yealink Configuration Encrypt Tool used to encrypt

provisioning documents was leaked leading to a compromise of confidentiality of provisioning documents.

- [Link](#)

—

” “Wed, 21 Feb 2024

Ivanti Connect Secure Unauthenticated Remote Code Execution

This Metasploit module chains a server side request forgery (SSRF) vulnerability (CVE-2024-21893) and a command injection vulnerability (CVE-2024-21887) to exploit vulnerable instances of either Ivanti Connect Secure or Ivanti Policy Secure, to achieve unauthenticated remote code execution. All currently supported versions 9.x and 22.x are vulnerable, prior to the vendor patch released on Feb 1, 2024. It is unknown if unsupported versions 8.x and below are also vulnerable.

- [Link](#)

—

” “Wed, 21 Feb 2024

WordPress 6.4.3 Username Disclosure

WordPress versions 6.4.3 and below appear to suffer from a REST API related username disclosure vulnerability.

- [Link](#)

—

” “Wed, 21 Feb 2024

Fuelflow 1.0 SQL Injection

Fuelflow version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Wed, 21 Feb 2024

ITFlow Cross Site Request Forgery

ITFlow versions prior to commit 432488eca3998c5be6b6b9e8f8ba01f54bc12378 suffer from a cross site request forgery vulnerability.

- [Link](#)

—

” “Wed, 21 Feb 2024

WEBIgniter 28.7.23 Cross Site Scripting

WEBIgniter version 28.7.23 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 20 Feb 2024

Kafka UI 0.7.1 Command Injection

A command injection vulnerability exists in Kafka UI versions 0.4.0 through 0.7.1 that allows an atta-

cker to inject and execute arbitrary shell commands via the groovy filter parameter at the topic section.

- [Link](#)

—

” “Tue, 20 Feb 2024

Savsoft Quiz 6.0 Enterprise Cross Site Scripting

Savsoft Quiz version 6.0 Enterprise suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 20 Feb 2024

SPA-CART CMS 1.9.0.3 Cross Site Scripting

SPA-CART CMS version 1.9.0.3 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 20 Feb 2024

Petrol Pump Management Software 1.0 Shell Upload

Petrol Pump Management Software version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Tue, 20 Feb 2024

Tourism Management System 2.0 Shell Upload

Tourism Management System version 2.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Backdoor_JS.Relvlshe.A Detection / Mitigation Bypass

Back in 2022, the researcher released a proof of concept to bypass the Backdoor:JS/Relvlshe.A detection in Windows Defender but it no longer works as it was mitigated. However, adding a simple javascript try catch error statement and eval'ing the hex string, it executes as of the time of this post.

- [Link](#)

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Trojan.Win32/Powessere.G VBScript Detection Bypass

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass. This issue was addressed. The fix was short lived as the researcher found yet another third trivial bypass. Previously, the researcher disclosed 3 bypasses

using rundll32 javascript, but this example leverages the VBSCRIPT and ActiveX engines.

- [Link](#)

—

” “Mon, 19 Feb 2024

InstantCMS 2.16.1 Cross Site Scripting

InstantCMS version 2.16.1 suffers from a persistent cross site scripting vulnerability that appears to require administrative access.

- [Link](#)

—

” “Mon, 19 Feb 2024

SureMDM On-Premise CAPTCHA Bypass / User Enumeration

SureMDM On-Premise versions prior to 6.31 suffer from CAPTCHA bypass and user enumeration vulnerabilities.

- [Link](#)

—

” “Mon, 19 Feb 2024

Online Library Management System 3 Password Reset

Online Library Management System version 3 suffers from a password reset vulnerability due to a logic flaw of allowing the same email address to be set for multiple users.

- [Link](#)

—

” “Mon, 19 Feb 2024

Employee Management System 1.0 SQL Injection

Employee Management System version 1.0 suffers from a remote SQL injection vulnerability. Original discovery of this finding is attributed to Ozlem Balci in January of 2024.

- [Link](#)

—

” “Mon, 19 Feb 2024

Chrome chrome.pageCapture.saveAsMHTML() Extension API Blocked Origin Bypass

Chrome has an issue where the chrome.pageCapture.saveAsMHTML() extension API can be used on blocked origins due to a racy access check.

- [Link](#)

—

” “Mon, 19 Feb 2024

WonderCMS 4.3.2 Cross Site Scripting / Remote Code Execution

WonderCMS version 4.3.2 remote exploit that leverages cross site scripting to achieve remote code execution.

- [Link](#)

—
” “Mon, 19 Feb 2024

User Registration And Login And User Management System 3.1 SQL Injection

User Registration and Login and User Management System version 3.1 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Detection Bypass Part 3

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass. This issue was addressed. The fix was short lived as the researcher has found yet another third trivial bypass.

- [Link](#)

—

” “Mon, 19 Feb 2024

JFrog Artifactory SQL Injection

JFrog Artifactory versions prior to 7.25.4 suffer from a remote blind SQL injection vulnerability.

- [Link](#)

—

” “Thu, 15 Feb 2024

Metabase 0.46.6 Remote Code Execution

Metabase version 0.46.6 pre-authentication remote code execution exploit.

- [Link](#)

—

” “Thu, 15 Feb 2024

DS Wireless Communication Code Execution

Proof of concept code for a flaw in DS Wireless Communication (DWC) with DWC_VERSION_3 and DWC_VERSION_11 that allows remote attackers to execute arbitrary code on a game-playing client's machine via a modified GPCM message.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 21 Feb 2024

ZDI-24-192: Schneider Electric EcoStruxure IT Gateway Hard-Coded Credentials Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-191: Schneider Electric EcoStruxure IT Gateway Hard-Coded Credentials Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-190: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-189: Trimble SketchUp SKP File Parsing Use-After-Free Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-188: Trimble SketchUp SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-187: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-186: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-185: Inductive Automation Ignition getJavaExecutable Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-184: Inductive Automation Ignition getParams Argument Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 21 Feb 2024

ZDI-24-183: Apache OFBiz createRegister Error Message Information Disclosure Vulnerability

- [Link](#)

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Zahnbürsten DDoS und bald hat Ivanti die OWASP Top 10 voll...



[Zum Youtube Video](#)

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-20	Berliner Hochschule für Technik (BHT)	[DEU]	Link
2024-02-20	Continental Aerospace	[USA]	Link
2024-02-18	Evangelische Landeskirche Hannovers	[DEU]	Link
2024-02-17	GCA (Charles André)	[FRA]	Link
2024-02-16	Government Employees Pension Fund (GEPF)	[ZAF]	Link
2024-02-15	PSI	[DEU]	Link
2024-02-15	Vili's Family Bakery	[AUS]	Link
2024-02-14	JCT600	[GBR]	Link
2024-02-13	Aztech Global	[SGP]	Link
2024-02-13	Varta	[DEU]	Link
2024-02-13	Coeur d'Alene	[USA]	Link
2024-02-13	Act21	[FRA]	Link
2024-02-13	School District 67	[CAN]	Link
2024-02-12	MSH International	[CAN]	Link
2024-02-11	Centre hospitalier d'Armentières	[FRA]	Link
2024-02-11	Hipocrate Information System (HIS)	[ROU]	Link
2024-02-11	Clinique privée La Colline (groupe Hirslanden)	[CHE]	Link
2024-02-11	Consulting Radiologists Ltd.	[USA]	Link
2024-02-09	Office of Colorado State Public Defender	[USA]	Link
2024-02-07	Université de Central Missouri	[USA]	Link
2024-02-07	SouthState Bank	[USA]	Link
2024-02-07	Commune de Petersberg	[DEU]	Link
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	Link
2024-02-06	Commune de Kalmar	[SWE]	Link

Datum	Opfer	Land	Information
2024-02-06	Advania	[SWE]	Link
2024-02-06	Onclusive	[GBR]	Link
2024-02-06	Kind	[DEU]	Link
2024-02-05	Prudential Financial, Inc.	[USA]	Link
2024-02-05	Central Arkansas Library System (CALS)	[USA]	Link
2024-02-04	Northern Light Health	[USA]	Link
2024-02-04	Middletown Area School District	[USA]	Link
2024-02-02	Germantown	[USA]	Link
2024-02-02	Universität de Reykjavík	[ISL]	Link
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	Link
2024-02-02	Mairie de Korneuburg	[AUT]	Link
2024-02-02	Welch's	[USA]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	Link
2024-02-01	Minnesota State University-Moorhead (MSUM)	[USA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-22	[Worthen Industries [We're giving you one last chance to save your business]]	alphv	Link
2024-02-21	[KHSS (You have 3 days)]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-21	[Lancaster]	akira	Link
2024-02-21	[Desarrollo De Tecnologia y Sistemas Ltda]	akira	Link
2024-02-21	[HRTec Inc]	bianlian	Link
2024-02-21	[Marchassociates]	bianlian	Link
2024-02-21	[Austen Consultants]	alphv	Link
2024-02-21	[dasteam.ch]	blackbasta	Link
2024-02-21	[doneff.com]	threeam	Link
2024-02-21	[Helical Technology]	8base	Link
2024-02-21	[Axel Johnson]	8base	Link
2024-02-20	[INFINITIUSA.COM]	mogilevich	Link
2024-02-20	[River Delta Unified School District]	meow	Link
2024-02-20	[Finlay Screening & Crushing Systems]	hunters	Link
2024-02-20	[Raocala]	everest	Link
2024-02-20	[advancedprosolutions.com]	cactus	Link
2024-02-19	[loransrl]	qilin	Link
2024-02-19	[soco.be]	lockbit3	Link
2024-02-19	[se.com]	cactus	Link
2024-02-19	[First Professional Services]	bianlian	Link
2024-02-19	[aivi.it]	trisec	Link
2024-02-19	[ki.se]	trisec	Link
2024-02-18	[Compression Leasing Services]	dragonforce	Link
2024-02-18	[Westward 360]	dragonforce	Link
2024-02-08	[aeromechinc.com]	lockbit3	Link
2024-02-18	[carlfischer.com]	lockbit3	Link
2024-02-17	[Bimbo Bakeries]	medusa	Link
2024-02-07	[bucher-strauss.ch]	lockbit3	Link
2024-02-16	[delia.pl]	stormous	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-14	[bombaygrills.com]	stormous	Link
2024-02-14	[calcomp.co.th]	stormous	Link
2024-02-02	[Abelsantosyasoc.com.ar]	stormous	Link
2024-02-18	[VSP Dental]	alphv	Link
2024-02-17	[Greater Napanee]	hunters	Link
2024-02-17	[Tiete Automobile]	hunters	Link
2024-02-17	[Voice Technologies]	hunters	Link
2024-02-17	[Afttrp]	hunters	Link
2024-02-17	[Chicago Zoological Society]	hunters	Link
2024-02-17	[BS&B Safety Systems L.L.C]	hunters	Link
2024-02-17	[Wapiti Energy]	hunters	Link
2024-02-17	[PSI]	hunters	Link
2024-02-17	[CP Communications]	hunters	Link
2024-02-16	[Prudential Financial]	alphv	Link
2024-02-16	[LoanDepot]	alphv	Link
2024-02-16	[www.cogans.ie]	trisec	Link
2024-02-16	[The Chas. E. Phipps]	medusa	Link
2024-02-16	[BRONSTEIN-CARMONA.COM]	clop	Link
2024-02-14	[davidsbridal.com]	werewolves	Link
2024-02-16	[Réseau Ribé]	hunters	Link
2024-02-16	[BRAM Auto Group]	akira	Link
2024-02-16	[etisalat.ae]	lockbit3	Link
2024-02-16	[theclosingagent.com]	lockbit3	Link
2024-02-16	[spaldingssd.com]	lockbit3	Link
2024-02-16	[tormetal.cl]	lockbit3	Link
2024-02-16	[Concello de Teo]	hunters	Link
2024-02-16	[pacificaco.uk]	blackbasta	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-16	[Ribe-Groupe]	hunters	Link
2024-02-16	[Griffin Dewatering]	hunters	Link
2024-02-15	[Dobrowski Stafford & Pierce]	bianlian	Link
2024-02-15	[LD Davis]	play	Link
2024-02-15	[von Hagen]	play	Link
2024-02-15	[Norman, Fox]	play	Link
2024-02-15	[HR Ewell & Hy-tec]	play	Link
2024-02-15	[Mechanical Reps]	play	Link
2024-02-15	[Onclusive]	play	Link
2024-02-15	[MeerServices]	play	Link
2024-02-15	[DuBose Strapping]	play	Link
2024-02-15	[SilverLining]	play	Link
2024-02-15	[Schuster Trucking Company]	hunters	Link
2024-02-15	[Asam]	akira	Link
2024-02-15	[Advantage Orthopedic & Sports Medicine Clinic]	bianlian	Link
2024-02-12	[Rush Energy Services Inc [Time's up]]	alphv	Link
2024-02-13	[Hawbaker Engineering]	snatch	Link
2024-02-15	[ASP BasilicataASM MateraIRCCS CROB]	rhysida	Link
2024-02-15	[champion.com.co]	lockbit3	Link
2024-02-15	[coreengg.com]	lockbit3	Link
2024-02-15	[sitrack.com]	lockbit3	Link
2024-02-15	[hatsinteriors.com]	lockbit3	Link
2024-02-15	[pradiergranulats.fr]	lockbit3	Link
2024-02-15	[centralepaysanne.lu]	lockbit3	Link
2024-02-15	[ASA Electronics [2.7 TB]]	alphv	Link
2024-02-14	[studiogalbusera.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-14	[Nekoosa School District]	akira	Link
2024-02-14	[BM Catalysts bmcatalysts.co.uk]	mydata	Link
2024-02-14	[vanwingerden.com]	abyss	Link
2024-02-14	[KALEEDS]	qilin	Link
2024-02-14	[conseguros]	qilin	Link
2024-02-14	[kabat.pl]	lockbit3	Link
2024-02-13	[Sindicato de Enfermería (SATSE)]	hunters	Link
2024-02-13	[wsnelson.com]	lockbit3	Link
2024-02-13	[fultoncountyga.gov]	lockbit3	Link
2024-02-14	[UNIFER]	8base	Link
2024-02-14	[Institutional Casework, Inc]	8base	Link
2024-02-14	[ATB SA Ingénieurs-conseils SIA]	8base	Link
2024-02-14	[mmiculinary.com]	lockbit3	Link
2024-02-12	[adioscancer.com]	lockbit3	Link
2024-02-14	[giraud]	qilin	Link
2024-02-13	[rajawali.com]	lockbit3	Link
2024-02-13	[motilaloswal.com]	lockbit3	Link
2024-02-13	[barberemerson.com]	blackbasta	Link
2024-02-13	[ffppkg.co.uk]	blackbasta	Link
2024-02-13	[patriziapepe.com]	blackbasta	Link
2024-02-13	[btl.info]	blackbasta	Link
2024-02-13	[globalrescue.com]	blackbasta	Link
2024-02-13	[ssmnlaw.com]	blackbasta	Link
2024-02-13	[leonardssyrups.com]	blackbasta	Link
2024-02-13	[ROOSENS BÉTONS]	qilin	Link
2024-02-13	[universalservicesms.com]	lockbit3	Link
2024-02-13	[Communication Federal Credit Union]	hunters	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-13	[doprastav.sk]	lockbit3	Link
2024-02-13	[The Source]	alphv	Link
2024-02-13	[ArcisGolf]	alphv	Link
2024-02-13	[Trans-Northern Pipelines]	alphv	Link
2024-02-13	[Herrs]	alphv	Link
2024-02-13	[Procopio]	alphv	Link
2024-02-13	[New Indy Containerboard]	alphv	Link
2024-02-13	[auruminstitute.org]	lockbit3	Link
2024-02-10	[SOPEM]	hunters	Link
2024-02-13	[Satse]	hunters	Link
2024-02-13	[Sanok Rubber CompanySpółka Akcyjna]	akira	Link
2024-02-12	[garonproducts.com]	threeam	Link
2024-02-07	[tecasrl.it]	lockbit3	Link
2024-02-12	[Antunovich Associates]	blacksuit	Link
2024-02-12	[DHX–Dependable Hawaiian Express]	knight	Link
2024-02-12	[Forgepresion.com]	cloak	Link
2024-02-12	[Rush Energy Services Inc [You have 48 hours]]	alphv	Link
2024-02-12	[SERCIDE]	alphv	Link
2024-02-12	[Lower Valley Energy, Inc]	alphv	Link
2024-02-12	[Modern Kitchens]	medusa	Link
2024-02-12	[vhprimary.com]	lockbit3	Link
2024-02-12	[germaintoiture.fr]	lockbit3	Link
2024-02-12	[Disaronno International]	meow	Link
2024-02-12	[Allmetal Inc.]	meow	Link
2024-02-12	[Freedom Munitions]	meow	Link
2024-02-12	[Arlington Perinatal Associates]	meow	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-12	[jacksonvillebeach.org]	lockbit3	Link
2024-02-12	[robs.org]	lockbit3	Link
2024-02-12	[parkhomeassist.co.uk]	lockbit3	Link
2024-02-12	[grotonschoools.org]	lockbit3	Link
2024-02-12	[isspol.gov]	lockbit3	Link
2024-02-12	[lyon.co.uk]	lockbit3	Link
2024-02-12	[dienerprecisionpumps.com]	lockbit3	Link
2024-02-12	[envie.org]	lockbit3	Link
2024-02-12	[sealco-leb.com]	lockbit3	Link
2024-02-12	[camarotto.it]	lockbit3	Link
2024-02-12	[paltertonprimary.co.uk]	lockbit3	Link
2024-02-12	[fidcornelis.be]	lockbit3	Link
2024-02-12	[plexustelerad.com]	lockbit3	Link
2024-02-12	[cabc.com.ar]	lockbit3	Link
2024-02-12	[textiles.org.tw]	lockbit3	Link
2024-02-12	[silverairways.com]	lockbit3	Link
2024-02-12	[Kreyenhop & Kluge]	hunters	Link
2024-02-12	[Kadac Australia]	medusa	Link
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	Link
2024-02-11	[lacolline-skincare.com]	lockbit3	Link
2024-02-10	[Upper Merion Township]	qilin	Link
2024-02-10	[YKP LTDA]	ransomhub	Link
2024-02-10	[Village of Skokie]	hunters	Link
2024-02-10	[Lancaster County Sheriff's Office]	hunters	Link
2024-02-10	[Nastech]	hunters	Link
2024-02-10	[Benchmark Management Group]	hunters	Link
2024-02-10	[SOPEM Tunisie]	hunters	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-10	[Impact Energy Services]	hunters	Link
2024-02-10	[Groupe Goyette]	hunters	Link
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	Link
2024-02-10	[Carespring Health Care]	hunters	Link
2024-02-10	[Avianor Aircraft]	hunters	Link
2024-02-10	[mranet.org]	abyss	Link
2024-02-10	[aisg-online.com]	lockbit3	Link
2024-02-10	[maddockhenson]	alphv	Link
2024-02-10	[verdimed.es]	lockbit3	Link
2024-02-10	[Pacific American Fish Company Inc.]	incransom	Link
2024-02-09	[water.cc]	lockbit3	Link
2024-02-09	[CTSI]	bianlian	Link
2024-02-09	[J.P. Original]	bianlian	Link
2024-02-09	[TechNet Kronoberg AB]	bianlian	Link
2024-02-09	[Capozzi Adler, P.C.]	bianlian	Link
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	Link
2024-02-09	[Grace Lutheran Foundation]	alphv	Link
2024-02-09	[ZGEO]	qilin	Link
2024-02-09	[alfiras.com]	lockbit3	Link
2024-02-09	[wannago.cloud]	qilin	Link
2024-02-09	[grupomoraval.com]	lockbit3	Link
2024-02-09	[cdtmedicus.pl]	lockbit3	Link
2024-02-09	[soken-ce.co.jp]	lockbit3	Link
2024-02-09	[maximumresearch.com]	lockbit3	Link
2024-02-09	[indoramaventures.com]	lockbit3	Link
2024-02-09	[willislease.com]	blackbasta	Link
2024-02-09	[northseayachtsupport.nl]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-09	[seymourct.org]	lockbit3	Link
2024-02-09	[bsaarchitects.com]	lockbit3	Link
2024-02-09	[moneyadvicetrust.org]	lockbit3	Link
2024-02-09	[posen.com]	abyss	Link
2024-02-09	[macqueeneq.com]	lockbit3	Link
2024-02-09	[parksite.com]	cactus	Link
2024-02-07	[galbusera.it]	lockbit3	Link
2024-02-08	[Ducont]	hunters	Link
2024-02-08	[perkinsmfg.com]	lockbit3	Link
2024-02-08	[originalfootwear.com]	lockbit3	Link
2024-02-08	[Jewish Home Lifecare]	alphv	Link
2024-02-08	[Distecna]	akira	Link
2024-02-07	[Western Municipal Construction]	blacksuit	Link
2024-02-07	[Southwest Binding & Laminating]	blacksuit	Link
2024-02-07	[TeraGo]	akira	Link
2024-02-07	[transaxle.com]	abyss	Link
2024-02-07	[Anderco PTE LTD]	8base	Link
2024-02-07	[Tetrosyl Group Limited]	8base	Link
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	Link
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link
2024-02-06	[axsbolivia.com]	lockbit3	Link
2024-02-06	[vimarequipment.com]	lockbit3	Link
2024-02-06	[deltron.com]	abyss	Link
2024-02-06	[B&B Electric Inc]	bianlian	Link
2024-02-06	[AVer Information]	akira	Link
2024-02-06	[Celeste]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-06	[ArpuPlus]	medusa	Link
2024-02-06	[gocco.com]	cactus	Link
2024-02-06	[spbglobal.com]	cactus	Link
2024-02-05	[Modern Kitchens]	play	Link
2024-02-05	[Greenwich Leisure]	play	Link
2024-02-05	[Ready Mixed Concrete]	play	Link
2024-02-05	[Northeastern Sheet Metal]	play	Link
2024-02-05	[Hannon Transport]	play	Link
2024-02-05	[McMillan Pazdan Smith]	play	Link
2024-02-05	[Mason Construction]	play	Link
2024-02-05	[Albert Bartlett]	play	Link
2024-02-05	[Perry-McCall Construction]	play	Link
2024-02-05	[Virgin Islands Lottery]	play	Link
2024-02-05	[Premier Facility Management]	play	Link
2024-02-05	[Douglas County Libraries]	play	Link
2024-02-05	[Leaders Staffing]	play	Link
2024-02-06	[asecos.com]	blackbasta	Link
2024-02-05	[GRUPO SCA[Release of all data]]	knight	Link
2024-02-05	[themisbourne.co.uk]	lockbit3	Link
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link
2024-02-05	[hutchpaving.com]	lockbit3	Link
2024-02-05	[davis-french-associates.co.uk]	lockbit3	Link
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	Link
2024-02-05	[VCS Observation]	akira	Link
2024-02-05	[noe.wifi.at]	lockbit3	Link
2024-02-05	[ksa-architecture.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-05	[GRTC Transit System]	bianlian	Link
2024-02-05	[semesco.com]	lockbit3	Link
2024-02-05	[ultraflexx.com]	lockbit3	Link
2024-02-05	[tgestiona.br]	lockbit3	Link
2024-02-05	[philogen.com]	lockbit3	Link
2024-02-05	[prima.com]	lockbit3	Link
2024-02-05	[logtainer.com]	lockbit3	Link
2024-02-05	[portline.pt]	lockbit3	Link
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link
2024-02-02	[Innovex Downhole Solutions]	play	Link
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	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.