# Cybersecurity Morgenreport


Ausgabe: 20230917

# Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

# Security-News

## Heise - Security-Alert

***Jetzt patchen! Sicherheitslösungen von Fortinet als Sicherheitsrisiko***
Mehrere Produkte von Fortinet sind verwundbar. Sicherheitsupdates schaffen Abhilfe.
- Link
—

***Management-Controller Lenovo XCC: Angreifer können Passwörter manipulieren***
Der Computerhersteller Lenovo hat in XClarity Controller mehrere Sicherheitslücken geschlossen.
- Link
—

***Sicherheitsupdates: Schadcode-Schlupflöcher in Foxit PDF geschlossen***
Angreifer können Windows-Systeme mit Foxit PDF Editor oder Foxit PDF Reader attackieren.
- Link
—

***Notfallpatch sichert Firefox und Thunderbird gegen Attacken ab***
Mozilla hat in seinen Webbrowsern und seinem Mailclient eine Sicherheitslücke geschlossen, die Angreifer bereits ausnutzen.
- Link
—

***Patchday: Angriffe mittels präparierter PDF-Dateien auf Adobe Acrobat***
Adobe hat in Acrobat und Reader, Connect und Experience Manager mehrere Sicherheitslücken geschlossen.
- Link
—

***Patchday: Angreifer attackieren unter anderem Microsoft Word***
Microsoft hat für Windows & Co. wichtige Sicherheitsupdates veröffentlicht. Zwei Lücken nutzen Angreifer bereits aus.
- Link
—

***Patchday: SAP schließt kritische Datenleak-Lücke in BusinessObjects***
Es sind wichtige Sicherheitsupdates für SAP-Software erschienen. Admins sollten zeitnah handeln.
- Link
—

***Jetzt patchen! Attacken auf kritische Schadcode-Lücke in Chrome naheliegend***
Google warnt vor Exploitcode für eine Schwachstelle in Chrome. Eine abgesicherte Version des Webbrowsers ist verfügbar.
- Link
—

***HPE OneView: Kritische Lücke erlaubt Umgehung von Authentifizierung***
HPE warnt vor mehreren Sicherheitslücken in OneView, einer Infrastrukturverwaltungssoftware. Angreifer könnten etwa die Anmeldung umgehen.
- Link
—

***Sicherheitslücken: Notepad++ gegen Schadcode-Attacken abgesichert***
In der aktuellen Version des freien Texteditors für Windows hat der Entwickler mehrere Sicherheitsprobleme gelöst.
- Link
—

# Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

## EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

**CVEs mit hoher Exploit-Wahrscheinlichkeit**

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-39143 | 0.921370000 | 0.985870000 | Link |
| CVE-2023-38035 | 0.973270000 | 0.998150000 | Link |
| CVE-2023-3519 | 0.911990000 | 0.984970000 | Link |
| CVE-2023-35078 | 0.965240000 | 0.994270000 | Link |
| CVE-2023-34362 | 0.936790000 | 0.987890000 | Link |
| CVE-2023-33246 | 0.971460000 | 0.997030000 | Link |
| CVE-2023-32315 | 0.973180000 | 0.998100000 | Link |
| CVE-2023-28771 | 0.926550000 | 0.986480000 | Link |
| CVE-2023-28121 | 0.937820000 | 0.988020000 | Link |
| CVE-2023-27524 | 0.964400000 | 0.993910000 | Link |
| CVE-2023-27372 | 0.970960000 | 0.996750000 | Link |
| CVE-2023-27350 | 0.970860000 | 0.996710000 | Link |
| CVE-2023-26469 | 0.910820000 | 0.984840000 | Link |
| CVE-2023-26360 | 0.904380000 | 0.984210000 | Link |
| CVE-2023-25717 | 0.965660000 | 0.994500000 | Link |
| CVE-2023-25194 | 0.924830000 | 0.986240000 | Link |
| CVE-2023-24489 | 0.974500000 | 0.999190000 | Link |
| CVE-2023-21839 | 0.960800000 | 0.992730000 | Link |
| CVE-2023-21823 | 0.907830000 | 0.984540000 | Link |
| CVE-2023-21554 | 0.961360000 | 0.992870000 | Link |
| CVE-2023-20887 | 0.954150000 | 0.991120000 | Link |
| CVE-2023-0669 | 0.965780000 | 0.994530000 | Link |

---

## BSI - Warn- und Informationsdienst (WID)

Fri, 15 Sep 2023
***[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation***
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten***
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit

Administratorrechten auszuführen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Mozilla Firefox: 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

—

Fri, 15 Sep 2023
***[NEU] [hoch] IBM Operational Decision Manager: Mehrere Schwachstellen***
Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in IBM Operational Decision Manager ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Samba: Mehrere Schwachstellen***
Ein entfernter, authetisierter oder anonymer Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, seine Rechte zu erweitern und die Domäne vollständig zu kompromittieren.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.
- Link

—

Fri, 15 Sep 2023
***[NEU] [hoch] Red Hat Quarkus: Schwachstelle ermöglicht die Umgehung von Sicherheitsmaßnahmen oder die Verursachung eines Denial-of-Service-Zustands***
Ein entfernter anonymer Angreifer kann eine Schwachstelle in Red Hat Quarkus ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] JFrog Artifactory: Mehrere Schwachstellen***
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in JFrog Artifactory ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand auszulösen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung***
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und Oracle Linux ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Camunda: Schwachstelle ermöglicht Privilegieneskalation***
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Camunda ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsmaßnahmen zu umgehen.
- Link

—

Fri, 15 Sep 2023
***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] Red Hat OpenShift Service Mesh und Service Mesh Containers: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh und Service Mesh Containers, sowie Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Informationen offenzulegen.

- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] Kubernetes: Mehrere Schwachstellen***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Kubernetes ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen***

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Developer Tools ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen***

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Rechte zu erweitern.

- Link

—

Fri, 15 Sep 2023

***[UPDATE] [hoch] Proofpoint Insider Threat Management: Mehrere Schwachstellen***

Ein entfernter Angreifer kann mehrere Schwachstellen in Proofpoint Insider Threat Management ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder Dateien zu manipulieren.

- Link

—

Thu, 14 Sep 2023

***[NEU] [hoch] Wibu-Systems CodeMeter: Schwachstelle ermöglicht Privilegieneskalation***

Ein lokaler Angreifer kann eine Schwachstelle in Wibu-Systems CodeMeter ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 14 Sep 2023

***[NEU] [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

—

Thu, 14 Sep 2023

***[NEU] [hoch] Fortinet FortiOS: Schwachstelle ermöglicht Cross-Site Scripting***

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Fortinet FortiOS und Fortinet FortiProxy ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- Link

—

## Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 9/16/2023 | [Fedora 37 : redis (2023-0e9e7544df)] | critical |
| 9/16/2023 | [Fedora 38 : redis (2023-03422cb8de)] | critical |
| 9/16/2023 | [OracleVM 3.4 : kernel-uek (OVMSA-2023-0021)] | critical |
| 9/15/2023 | [Grafana Labs WebUI Default Credentials] | critical |
| 9/15/2023 | [NETGEAR ProSAFE Network Management System Authentication Bypass (CVE-2023-38096)] | critical |
| 9/15/2023 | [Golang 1.21.x < 1.21.1 RCE] | critical |
| 9/15/2023 | [Apache Solr 6.6.x < 6.6.7 / 7.x < 7.7.4 / 8.x < 8.6.3 Authentication Bypass (CVE-2020-13957)] | critical |
| 9/15/2023 | [Apache Solr 7.x < 7.7.4 / 8.x < 8.8.2 Multiple Vulnerabilities] | critical |
| 9/16/2023 | [Fedora 37 : libwebp (2023-3388038193)] | high |
| 9/16/2023 | [Fedora 38 : golang (2023-aad8537873)] | high |
| 9/16/2023 | [Fedora 38 : curl (2023-b1253907f1)] | high |
| 9/16/2023 | [Fedora 37 : flac (2023-bf8423a373)] | high |
| 9/16/2023 | [openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0247-1)] | high |
| 9/16/2023 | [SUSE SLES12 Security Update : MozillaFirefox (SUSE-SU-2023:3626-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 23 for SLE 15 SP3) (SUSE-SU-2023:3607-1)] | high |
| 9/16/2023 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:3610-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 37 for SLE 15 SP2) (SUSE-SU-2023:3621-1)] | high |
| 9/16/2023 | [SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 33 for SLE 15 SP1) (SUSE-SU-2023:3603-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 28 for SLE 15 SP3) (SUSE-SU-2023:3623-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 36 for SLE 15 SP2) (SUSE-SU-2023:3620-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 38 for SLE 15 SP2) (SUSE-SU-2023:3622-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : MozillaFirefox (SUSE-SU-2023:3609-1)] | high |
| 9/16/2023 | [SUSE SLES15 Security Update : kernel (Live Patch 29 for SLE 15 SP2) (SUSE-SU-2023:3612-1)] | high |
| 9/15/2023 | [SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3600-1)] | high |
| 9/15/2023 | [SUSE SLES12 Security Update : kernel (SUSE-SU-2023:3601-1)] | high |
| 9/15/2023 | [SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:3599-1)] | high |
| 9/15/2023 | [Fedora 38 : borgbackup (2023-555f9fac30)] | high |
| 9/15/2023 | [Fedora 37 : firefox (2023-31fe7ee034)] | high |
| 9/15/2023 | [Fedora 38 : firefox (2023-c7af372e2e)] | high |
| 9/15/2023 | [Fedora 37 : borgbackup (2023-34411d8f77)] | high |
| 9/15/2023 | [Fedora 38 : libwebp (2023-c4fa8a204d)] | high |
| 9/15/2023 | [Fedora 37 : python3-docs / python3.11 (2023-aeb32a843f)] | high |
| 9/15/2023 | [Docker Desktop < 4.6.0 DirtyPipe] | high |
| 9/15/2023 | [Docker Desktop for Windows < 4.6.0 DirtyPipe] | high |
| 9/15/2023 | [Golang < 1.20.8 / 1.21.x < 1.21.1 Multiple Vulnerabilities] | high |
| 9/15/2023 | [Docker Desktop < 4.6.0 Improper Link Resolution] | high |
| 9/15/2023 | [Docker Desktop < 2.3.0.2 Privilege Escalation] | high |
| 9/15/2023 | [Docker Desktop < 4.5.0 Incorrect Access Control] | high |
| 9/15/2023 | [Oracle Linux 9 : kernel (ELSA-2023-5069)] | high |
| 9/15/2023 | [Apache Solr < 8.6.0 Information Disclosure (CVE-2020-13941)] | high |

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 9/15/2023 | [Microsoft Edge (Chromium) < 117.0.2045.31 (CVE-2023-4863)] | high |

# Aktiv ausgenutzte Sicherheitslücken

## Exploits

“Fri, 15 Sep 2023
***Academy LMS 6.2 SQL Injection***
Academy LMS version 6.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Fri, 15 Sep 2023
***Academy LMS 6.2 Cross Site Scripting***
Academy LMS version 6.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Fri, 15 Sep 2023
***Italia Mediasky CMS 2.0 Cross Site Scripting***
Italia Mediasky CMS version 2.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Fri, 15 Sep 2023
***Italia Mediasky CMS 2.0 Cross Site Request Forgery***
Italia Mediasky CMS version 2.0 suffers from a cross site request forgery vulnerability.
- Link
—
” “Fri, 15 Sep 2023
***Chrome Read-Only Property Overwrite***
Chrome suffers from a read-only property overwrite in TurboFan.
- Link
—
” “Thu, 14 Sep 2023
***Windows Common Log File System Driver (clfs.sys) Privilege Escalation***
A privilege escalation vulnerability exists in the clfs.sys driver which comes installed by default on Windows 10 21H2, Windows 11 21H2 and Windows Server 20348 operating systems. This Metasploit module exploit makes use to two different kinds of specially crafted .blf files.
- Link
—
” “Thu, 14 Sep 2023
***iSmile Soft CMS 0.3.0 Add Administrator***
iSmile Soft CMS version 0.3.0 suffers from an add administrator vulnerability.
- Link
—
” “Thu, 14 Sep 2023
***islamnt CMS 2.1.0 Add Administrator***
islamnt CMS version 2.1.0 suffers from an add administrator vulnerability.
- Link
—
” “Thu, 14 Sep 2023
***islamnt CMS 2.1.0 Cross Site Scripting***
islamnt CMS version 2.1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 14 Sep 2023
***Night Club Booking Software 1.0 Cross Site Scripting***
Night Club Booking Software version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 14 Sep 2023
***ImgHosting 1.3 Cross Site Scripting***
ImgHosting version 1.3 suffers from a cross site scripting vulnerability.
- Link
—

” “Wed, 13 Sep 2023
***Ivanti Sentry Authentication Bypass / Remote Code Execution***
This Metasploit module exploits an authentication bypass in Ivanti Sentry which exposes API functionality which allows for code execution in the context of the root user.
- Link
—
” “Wed, 13 Sep 2023
***PHP Shopping Cart 4.2 SQL Injection***
PHP Shopping Cart version 4.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 13 Sep 2023
***Fundraising Script 1.0 SQL Injection***
Fundraising Script version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 13 Sep 2023
***Blood Bank And Donor Management System 2.2 Cross Site Scripting***
Blood Bank and Donor Management System version 2.2 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Wed, 13 Sep 2023
***Kleeja 1.5.4 Cross Site Scripting***
Kleeja version 1.5.4 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 13 Sep 2023
***K-LOANS 1.4.5 Insecure Settings***
K-LOANS version 1.4.5 suffers from an ignored default credential vulnerability.
- Link
—
” “Tue, 12 Sep 2023
***Equipment Rental Script 1.0 SQL Injection***
Equipment Rental Script version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 12 Sep 2023
***Kolifa Download CMS 1.2 HTML Injection***
Kolifa Download CMS version 1.2 suffers from an html injection vulnerability.
- Link
—
” “Tue, 12 Sep 2023
***KALIMATAN GMS 1.0.0 Cross Site Scripting***
KALIMATAN GMS version 1.0.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 12 Sep 2023
***Kylin CMS 1.3.0 SQL Injection***
Kylin CMS version 1.3.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Tue, 12 Sep 2023
***Kaledo RD CMS 1.0 SQL Injection***
Kaledo RD CMS version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 11 Sep 2023
***WordPress Slimstat Analytics 5.0.9 Cross Site Scripting / SQL Injection***
WordPress Slimstat Analytics plugin versions 5.0.9 and below suffer from cross site scripting and remote SQL injection vulnerabilities.
- Link

—
” “Mon, 11 Sep 2023
***VMware vRealize Log Insight Unauthenticated Remote Code Execution***
VMware vRealize Log Insights versions 8.x contain multiple vulnerabilities, such as directory traversal, broken access control, deserialization, and information disclosure. When chained together, these vulnerabilities allow a remote, unauthenticated attacker to execute arbitrary commands on the underlying operating system as the root user. This Metasploit module achieves code execution via triggering a RemotePakDownloadCommand command via the exposed thrift service after obtaining the node token by calling a GetConfigRequest thrift command. After the download, it will trigger a PakUpgradeCommand for processing the specially crafted PAK archive, which then will place the JSP payload under a certain API endpoint (pre-authenticated) location upon extraction for gaining remote code execution. Successfully tested against version 8.0.2.
- Link
—
” “Mon, 11 Sep 2023
***Splunk Enterprise Account Takeover***
Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14 allows low-privileged users who hold a role with edit_user capability assigned to it the ability to escalate their privileges to that of the admin user by providing specially crafted web requests.
- Link
—
”

## 0-Day

## Die Hacks der Woche

mit Martin Haunschmid

**Schlechte Neuigkeiten: LastPass Tresore geknackt? UND: Wie der Microsoft Signing Key verschwand**


Zum Youtube Video

## Cyberangriffe: (Sep)

| Datum | Opfer | Land | Information |
|---|---|---|---|
| 2023-09-14 | Auckland Transport | [NZL] | Link |
| 2023-09-12 | Un prestataire de Pelmorex Corp. | [CAN] | Link |
| 2023-09-12 | IFX Networks | [COL] | Link |
| 2023-09-11 | MGM Resorts | [USA] | Link |
| 2023-09-11 | Partenaire de moBiel | [DEU] | Link |
| 2023-09-11 | Le système d'information judiciaire régional (REJIS) du comté de St. Louis | [USA] | Link |
| 2023-09-11 | Zetema Progetto Cultura | [ITA] | Link |
| 2023-09-07 | Le groupe hospitalier Saint-Vincent à Strasbourg | [FRA] | Link |
| 2023-09-06 | L'académie St Augustine à Maidstone | [GBR] | Link |
| 2023-09-06 | Comté de Hinds | [USA] | Link |
| 2023-09-06 | ORBCOMM | [USA] | Link |
| 2023-09-05 | Mairie de Séville | [ESP] | Link |
| 2023-09-05 | Financial Services Commission (FSC) | [JAM] | Link |
| 2023-09-05 | Decatur Independent School District (DISD) | [USA] | Link |
| 2023-09-05 | Thermae 2000 | [NLD] | Link |
| 2023-09-04 | Maiden Erlegh Trust | [GBR] | Link |
| 2023-09-01 | Comitato Elettrotecnico Italiano (CEI) | [ITA] | Link |
| 2023-09-01 | Secrétariat de l'environnement et des ressources naturelles (Semarnat) | [MEX] | Link |

## Ransomware-Erpressungen: (Sep)

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2023-09-16 | [TransTerra] | cyphbit | Link |
| 2023-09-16 | [Marston Domsel] | cyphbit | Link |
| 2023-09-16 | [tuvsud.com] | lockbit3 | Link |
| 2023-09-16 | [perfectlaw.com] | lockbit3 | Link |
| 2023-09-16 | [beamconstruction.com] | lockbit3 | Link |
| 2023-09-16 | [scottpartners.com] | lockbit3 | Link |
| 2023-09-16 | [eljayoil.com] | lockbit3 | Link |
| 2023-09-16 | [dasholding.ae] | lockbit3 | Link |
| 2023-09-16 | [faithfamilyacademy.org] | lockbit3 | Link |
| 2023-09-16 | [syntech.com.sg] | lockbit3 | Link |
| 2023-09-16 | [piramidal.com.br] | lockbit3 | Link |
| 2023-09-16 | [tlip2.com] | lockbit3 | Link |
| 2023-09-16 | [energyinsight.co.za] | lockbit3 | Link |
| 2023-09-16 | [mehmetceylanyapi.com.tr] | lockbit3 | Link |
| 2023-09-16 | [aeroportlleida.cat] | lockbit3 | Link |
| 2023-09-16 | [lamaisonmercier.com] | lockbit3 | Link |
| 2023-09-16 | [neolaser.es] | lockbit3 | Link |
| 2023-09-16 | [commercialfluidpower.com] | lockbit3 | Link |
| 2023-09-16 | [glat.zapweb.co.il] | lockbit3 | Link |
| 2023-09-16 | [motsaot.co.il] | lockbit3 | Link |
| 2023-09-16 | [gsaenz.com.mx] | lockbit3 | Link |
| 2023-09-16 | [ipsenlogistics.com] | lockbit3 | Link |
| 2023-09-16 | [Financial Decisions] | alphv | Link |
| 2023-09-15 | [Updates: Israel “MYMC”] | ragnarlocker | Link |
| 2023-09-15 | [hollandspecial] | alphv | Link |
| 2023-09-15 | [pelicanwoodcliff.com] | lockbit3 | Link |
| 2023-09-15 | [hillsboroughschools.org] | lockbit3 | Link |
| 2023-09-15 | [Steelforce] | trigona | Link |
| 2023-09-14 | [wdgroup.com.my] | threeam | Link |
| 2023-09-14 | [pvbfabs.com] | threeam | Link |
| 2023-09-14 | [intechims.com] | threeam | Link |
| 2023-09-14 | [zero-pointorganics.com] | threeam | Link |
| 2023-09-14 | [visitingphysiciansnetwork.com] | threeam | Link |
| 2023-09-14 | [clearwaterlandscape.com] | threeam | Link |
| 2023-09-14 | [Statement on MGM Resorts International: Setting the record straight] | alphv | Link |
| 2023-09-14 | [etsi.uy] | knight | Link |
| 2023-09-14 | [Ja Quith Press Release] | monti | Link |
| 2023-09-14 | [East Baking Press Release] | monti | Link |
| 2023-09-14 | [American Steel & Aluminum] | akira | Link |
| 2023-09-14 | [Waterford Retirement Residence] | cyphbit | Link |
| 2023-09-14 | [Shelly Engineering Metal Work] | cyphbit | Link |
| 2023-09-14 | [Harmonic Accounting] | cyphbit | Link |
| 2023-09-14 | [Imperador S.R.L] | cyphbit | Link |
| 2023-09-14 | [Waterford Retirement Residence] | cyphbit | Link |
| 2023-09-14 | [Shelly Engineering Metal Work] | cyphbit | Link |
| 2023-09-14 | [RSV Centrale Bvba] | cyphbit | Link |
| 2023-09-14 | [Soprovise] | cyphbit | Link |
| 2023-09-14 | [carthagehospital.com] | lockbit3 | Link |
| 2023-09-07 | [Fondation Vincent De Paul] | noescape | Link |
| 2023-09-07 | [EDUCAL, SA de CV] | noescape | Link |
| 2023-09-13 | [Enpos] | stormous | Link |
| 2023-09-13 | [clearcreek.org] | lockbit3 | Link |
| 2023-09-13 | [Financial Services Commission] | blacksuit | Link |
| 2023-09-13 | [Cedar Holdings] | trigona | Link |
| 2023-09-13 | [Benefit Management INC] | knight | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2023-09-13 | [Dpc & S] | play | Link |
| 2023-09-13 | [Carpet One] | play | Link |
| 2023-09-13 | [Markentrainer Werbeagentur, Elwema Automotive] | play | Link |
| 2023-09-13 | [Tanachira Group] | knight | Link |
| 2023-09-12 | [Accuride] | akira | Link |
| 2023-09-12 | [Abbeyfield] | incransom | Link |
| 2023-09-12 | [Morgan Smith Industries LLC] | knight | Link |
| 2023-09-12 | [Decarie Motors Inc] | knight | Link |
| 2023-09-12 | [sinloc.com] | lockbit3 | Link |
| 2023-09-12 | [M-Extend / MANIP] | alphv | Link |
| 2023-09-12 | [Dee Sign] | lorenz | Link |
| 2023-09-12 | [Credifiel was hacked and a lot of personal customer and financial information was stolen] | alphv | Link |
| 2023-09-12 | [Derrimon Trading was hacked. Critical data of the company and its customers was stolen] | alphv | Link |
| 2023-09-12 | [CORTEL Technologies] | qilin | Link |
| 2023-09-11 | [Alps Alpine] | blackbyte | Link |
| 2023-09-11 | [24/7 Express Logistics (Unpay-Start Leaking)] | ragroup | Link |
| 2023-09-07 | [International Joint Commission] | noescape | Link |
| 2023-09-02 | [Altmann Dental GmbH & Co KG] | noescape | Link |
| 2023-09-03 | [AdSage Technology Co., Ltd.] | noescape | Link |
| 2023-09-11 | [deeroaks.com] | lockbit3 | Link |
| 2023-09-11 | [Cmranallolaw.com] | everest | Link |
| 2023-09-11 | [Wardlaw Claims Service] | cactus | Link |
| 2023-09-11 | [Levine Bagade Han] | cactus | Link |
| 2023-09-11 | [Leekes] | cactus | Link |
| 2023-09-11 | [My Insurance Broker] | cactus | Link |
| 2023-09-11 | [Unimarketing] | cactus | Link |
| 2023-09-11 | [cfsigroup.ca] | lockbit3 | Link |
| 2023-09-11 | [Wave Hill] | medusa | Link |
| 2023-09-11 | [Steripharma ] | medusa | Link |
| 2023-09-11 | [co.grant.mn.us] | lockbit3 | Link |
| 2023-09-11 | [KUITS Solicitors] | alphv | Link |
| 2023-09-11 | [Ford Covesa] | 8base | Link |
| 2023-09-10 | [New Venture Escrow] | bianlian | Link |
| 2023-09-10 | [BOZOVICH TIMBER PRODUCTS INC] | mallox | Link |
| 2023-09-10 | [njsba.com] | abyss | Link |
| 2023-09-10 | [Singing River Health System] | rhysida | Link |
| 2023-09-10 | [Core Desktop] | rhysida | Link |
| 2023-09-09 | [Kirby Risk] | blackbyte | Link |
| 2023-09-09 | [airelec.bg] | ransomed | Link |
| 2023-09-09 | [pilini.bg] | ransomed | Link |
| 2023-09-09 | [kasida.bg] | ransomed | Link |
| 2023-09-09 | [proxy-sale.com] | ransomed | Link |
| 2023-09-09 | [IT-Center Syd] | rhysida | Link |
| 2023-09-08 | [www.northriverco.com] | abyss | Link |
| 2023-09-08 | [sd69.org] | lockbit3 | Link |
| 2023-09-08 | [milbermakris.com] | lockbit3 | Link |
| 2023-09-08 | [monaco-technologies.com] | lockbit3 | Link |
| 2023-09-08 | [UNIVERSAL REALTY GROUP] | 8base | Link |
| 2023-09-08 | [Geo Tek] | cactus | Link |
| 2023-09-08 | [hanwha.com] | lockbit3 | Link |
| 2023-09-08 | [Custom Powder Systems] | cactus | Link |
| 2023-09-08 | [JSS Almonds] | cactus | Link |
| 2023-09-08 | [atWork Office Furniture] | cactus | Link |
| 2023-09-08 | [BRiC Partnership] | cactus | Link |
| 2023-09-08 | [PAUL-ALEXANDRE DOICESCO] | qilin | Link |
| 2023-09-08 | [WACOAL] | qilin | Link |
| 2023-09-08 | [Linktera] | ransomed | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2023-09-07 | [24/7 Express Logistics ] | ragroup | Link |
| 2023-09-07 | [FOCUS Business Solutions] | blackbyte | Link |
| 2023-09-07 | [Chambersburg Area School District] | blackbyte | Link |
| 2023-09-07 | [Pvc-ms] | stormous | Link |
| 2023-09-07 | [toua.net] | lockbit3 | Link |
| 2023-09-07 | [Conselho Superior da Justiça do Trabalho] | 8base | Link |
| 2023-09-07 | [Sebata Holdings (MICROmega Holdings)] | bianlian | Link |
| 2023-09-07 | [TORMAX USA] | cactus | Link |
| 2023-09-07 | [West Craft Manufacturing] | cactus | Link |
| 2023-09-07 | [Trimaran Capital Partners] | cactus | Link |
| 2023-09-07 | [Specialised Management Services] | cactus | Link |
| 2023-09-06 | [nobleweb.com] | lockbit3 | Link |
| 2023-09-06 | [protosign.it] | lockbit3 | Link |
| 2023-09-06 | [concrejato.com.br] | lockbit3 | Link |
| 2023-09-06 | [meroso.be] | lockbit3 | Link |
| 2023-09-06 | [qsoftnet.com] | lockbit3 | Link |
| 2023-09-06 | [ragasa.com.mx] | lockbit3 | Link |
| 2023-09-06 | [I Keating Furniture World] | incransom | Link |
| 2023-09-06 | [onyx-fire.com] | lockbit3 | Link |
| 2023-09-06 | [gormanusa.com] | lockbit3 | Link |
| 2023-09-06 | [Israel Medical Center - leaked] | ragnarlocker | Link |
| 2023-09-06 | [It4 Solutions Robras] | incransom | Link |
| 2023-09-06 | [Smead] | blackbyte | Link |
| 2023-09-06 | [Solano-Napa Pet Emergency Clinic] | knight | Link |
| 2023-09-06 | [Ayass BioScience] | alphv | Link |
| 2023-09-06 | [Sabre Corporation] | dunghill_leak | Link |
| 2023-09-06 | [Energy One] | akira | Link |
| 2023-09-06 | [FRESH TASTE PRODUCE USA AND ASSOCIATES INC.] | 8base | Link |
| 2023-09-06 | [Chula Vista Electric (CVE)] | 8base | Link |
| 2023-09-05 | [Precisely, Winshuttle] | play | Link |
| 2023-09-05 | [Kikkerland Design] | play | Link |
| 2023-09-05 | [Markentrainer Werbeagentur] | play | Link |
| 2023-09-05 | [Master Interiors] | play | Link |
| 2023-09-05 | [Bordelon Marine] | play | Link |
| 2023-09-05 | [Majestic Spice] | play | Link |
| 2023-09-04 | [Infinity Construction Company] | noescape | Link |
| 2023-09-05 | [Maxxd Trailers] | cactus | Link |
| 2023-09-05 | [MINEMAN Systems] | cactus | Link |
| 2023-09-05 | [Promotrans] | cactus | Link |
| 2023-09-05 | [Seymours] | cactus | Link |
| 2023-09-02 | [Strata Plan Australia FULL LEAK] | alphv | Link |
| 2023-09-02 | [TissuPath Australia FULL LEAK] | alphv | Link |
| 2023-09-05 | [Marfrig Global Foods] | cactus | Link |
| 2023-09-05 | [Brooklyn Premier Orthopedics FULL LEAK!] | alphv | Link |
| 2023-09-05 | [Barry Plant LEAK!] | alphv | Link |
| 2023-09-05 | [Barsco] | cactus | Link |
| 2023-09-05 | [Foroni SPA] | cactus | Link |
| 2023-09-05 | [Hornsyld Købmandsgaard] | cactus | Link |
| 2023-09-05 | [Lagarde Meregnani] | cactus | Link |
| 2023-09-05 | [spmblaw.com] | lockbit3 | Link |
| 2023-09-05 | [Unimed] | trigona | Link |
| 2023-09-05 | [Cyberport] | trigona | Link |
| 2023-09-05 | [godbeylaw.com] | lockbit3 | Link |
| 2023-09-01 | [Firmdale Hotels] | play | Link |
| 2023-09-04 | [easydentalcare.us] | ransomed | Link |
| 2023-09-04 | [quantinuum.com] | ransomed | Link |
| 2023-09-04 | [laasr.eu] | ransomed | Link |
| 2023-09-04 | [medcenter-tambov.ru] | ransomed | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2023-09-04 | [makflix.eu] | ransomed | Link |
| 2023-09-04 | [nucleus.live] | ransomed | Link |
| 2023-09-04 | [wantager.com] | ransomed | Link |
| 2023-09-04 | [Zurvita ] | ragroup | Link |
| 2023-09-04 | [Piex Group ] | ragroup | Link |
| 2023-09-04 | [Yuxin Automobile Co.Ltd (  ) ] | ragroup | Link |
| 2023-09-02 | [Mulkay Cardiology Consultants] | noescape | Link |
| 2023-09-04 | [Balcan] | cactus | Link |
| 2023-09-04 | [Barco Uniforms] | cactus | Link |
| 2023-09-04 | [Swipe.bg] | ransomed | Link |
| 2023-09-04 | [Balmit Bulgaria] | ransomed | Link |
| 2023-09-04 | [cdwg.com] | lockbit3 | Link |
| 2023-09-04 | [Betton France] | medusa | Link |
| 2023-09-04 | [Jules B] | medusa | Link |
| 2023-09-04 | [VVandA] | 8base | Link |
| 2023-09-04 | [Prodegest Assessors] | 8base | Link |
| 2023-09-04 | [Knight Barry Title] | snatch | Link |
| 2023-09-03 | [phms.com.au] | ransomed | Link |
| 2023-09-03 | [paynesvilleareainsurance.com] | ransomed | Link |
| 2023-09-03 | [SKF.com] | ransomed | Link |
| 2023-09-03 | [gosslaw.com] | lockbit3 | Link |
| 2023-09-03 | [marianoshoes.com] | lockbit3 | Link |
| 2023-09-03 | [Arkopharma] | incransom | Link |
| 2023-09-02 | [Taylor University] | moneymessage | Link |
| 2023-09-03 | [Riverside Logistics] | moneymessage | Link |
| 2023-09-03 | [Estes Design & Manufacturing] | moneymessage | Link |
| 2023-09-03 | [Aiphone] | moneymessage | Link |
| 2023-09-03 | [DDB Unlimited (ddbunlimited.com)] | rancoz | Link |
| 2023-09-03 | [Rick Ramos Law (rickramoslaw.com)] | rancoz | Link |
| 2023-09-03 | [Newton Media A.S] | alphv | Link |
| 2023-09-03 | [Lawsonlundell] | alphv | Link |
| 2023-09-02 | [glprop.com] | lockbit3 | Link |
| 2023-09-02 | [Strata Plan Australia] | alphv | Link |
| 2023-09-02 | [TissuPath Australia] | alphv | Link |
| 2023-09-02 | [seasonsdarlingharbour.com.au] | lockbit3 | Link |
| 2023-09-02 | [nerolac.com] | lockbit3 | Link |
| 2023-09-02 | [ramlowstein.com] | lockbit3 | Link |
| 2023-09-02 | [Barry Plant Real Estate Australia] | alphv | Link |
| 2023-09-02 | [sterncoengineers.com] | lockbit3 | Link |
| 2023-09-02 | [attorneydanwinder.com] | lockbit3 | Link |
| 2023-09-02 | [designlink.us] | lockbit3 | Link |
| 2023-09-02 | [gh2.com] | lockbit3 | Link |
| 2023-09-02 | [DOIT - Canadian IT company allowed leak of its own clients.] | ragnarlocker | Link |
| 2023-09-02 | [SKF.com] | everest | Link |
| 2023-09-02 | [Powersportsmarketing.com] | everest | Link |
| 2023-09-02 | [Statefarm.com] | everest | Link |
| 2023-09-02 | [Aban Tether & OK exchange] | arvinclub | Link |
| 2023-09-02 | [cc-gorgesardeche.fr] | lockbit3 | Link |
| 2023-09-01 | [cciamp.com] | lockbit3 | Link |
| 2023-09-01 | [Templeman Consulting Group Inc] | bianlian | Link |
| 2023-09-01 | [vodatech.com.tr] | lockbit3 | Link |
| 2023-09-01 | [F???????? ?????s] | play | Link |
| 2023-09-01 | [Hawaii Health System] | ransomed | Link |
| 2023-09-01 | [hamilton-techservices.com] | lockbit3 | Link |
| 2023-09-01 | [aquinas.qld.edu.au] | lockbit3 | Link |
| 2023-09-01 | [konkconsulting.com] | lockbit3 | Link |
| 2023-09-01 | [Piex Group] | ragroup | Link |
| 2023-09-01 | [Yuxin Automobile Co.Ltd(  )] | ragroup | Link |

# Quellen

## Quellenverzeichnis


1) Cyberwatch - https://github.com/Casualtek/Cyberwatch
2) Ransomware.live - https://data.ransomware.live
3) Heise Security Alerts! - https://www.heise.de/security/alerts/
4) First EPSS - https://www.first.org/epss/
5) BSI WID - https://wid.cert-bund.de/
6) Tenable Plugins - https://www.tenable.com/plugins/
7) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

# Impressum

***Herausgeber:***
Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

***E-Mail***
info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.