



Ausgabe: 20230913

# 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

### ***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](#)

---

### ***NSO-Group-Angriff: Notfall-Updates für iPhone, iPad, Mac und Apple Watch***

Apple hat am Donnerstagabend nochmals Updates für seine aktuellen Betriebssysteme nachgeschoben. Enthalten sind Fixes für einen aktiven Exploit.

- [Link](#)

---

### ***Aruba-Controller und -Gateways mit hochriskanten Sicherheitslücken***

Für Aruba-Controller und -Gateways der Serien 9000 und 9200 gibt es Updates, die hochriskante Sicherheitslücken schließen.

- [Link](#)

---

### ***Sicherheitsupdates: Unbefugte Zugriffe auf TP-Link-Router möglich***

Angreifer können verschiedene Router von TP-Link attackieren und im schlimmsten Fall eigene Befehle auf Geräten ausführen.

- [Link](#)

---

### ***Cisco warnt vor teils kritischen Lücken und liefert Updates für mehrere Produkte***

In mehreren Cisco-Produkten lauern Sicherheitslücken, die Updates schließen sollen. Eine gilt sogar als kritisch.

- [Link](#)

---

### ***Patchday: Schadcode-Attacken auf Android 11, 12, 13 möglich***

Google und weitere Hersteller von Android-Geräten haben wichtige Sicherheitsupdates veröffentlicht. Eine Lücke wird bereits ausgenutzt.

- [Link](#)

---

### ***Sicherheitsupdates: Angreifer können Kontrolle über Asus-Router erlangen***

Mehrere Sicherheitslücken gefährden verschiedene Router-Modelle von Asus. Patches sichern Geräte ab.

- [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	0.985830000	<a href="#">Link</a>
CVE-2023-38035	0.960130000	0.992560000	<a href="#">Link</a>
CVE-2023-3519	0.911990000	0.984950000	<a href="#">Link</a>
CVE-2023-35078	0.965240000	0.994250000	<a href="#">Link</a>
CVE-2023-34362	0.936790000	0.987870000	<a href="#">Link</a>
CVE-2023-33246	0.971460000	0.997020000	<a href="#">Link</a>
CVE-2023-32315	0.973180000	0.998100000	<a href="#">Link</a>
CVE-2023-28771	0.926550000	0.986470000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987990000	<a href="#">Link</a>
CVE-2023-27372	0.970600000	0.996570000	<a href="#">Link</a>
CVE-2023-27350	0.970860000	0.996710000	<a href="#">Link</a>
CVE-2023-26469	0.910820000	0.984820000	<a href="#">Link</a>
CVE-2023-26360	0.908440000	0.984560000	<a href="#">Link</a>
CVE-2023-25717	0.965660000	0.994470000	<a href="#">Link</a>
CVE-2023-25194	0.924830000	0.986210000	<a href="#">Link</a>
CVE-2023-24489	0.974410000	0.999140000	<a href="#">Link</a>
CVE-2023-21839	0.960800000	0.992750000	<a href="#">Link</a>
CVE-2023-21823	0.907830000	0.984520000	<a href="#">Link</a>
CVE-2023-21554	0.954850000	0.991300000	<a href="#">Link</a>
CVE-2023-20887	0.954150000	0.991110000	<a href="#">Link</a>
CVE-2023-0669	0.965780000	0.994510000	<a href="#">Link</a>

## BSI - Warn- und Informationsdienst (WID)

Tue, 12 Sep 2023

### **[NEU] [hoch] SAP Patchday September 2023**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Tue, 12 Sep 2023

### **[NEU] [hoch] Nagios Enterprises Nagios XI: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Nagios Enterprises Nagios XI ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten oder um Daten zu manipulieren.

- [Link](#)

---

Tue, 12 Sep 2023

**[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen**

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

- [Link](#)

---

Tue, 12 Sep 2023

**[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

---

Tue, 12 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](#)

---

Tue, 12 Sep 2023

**[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Nvidia Treibern ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen, seine Privilegien zu erweitern und Daten zu manipulieren.

- [Link](#)

---

Tue, 12 Sep 2023

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

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

- [Link](#)

---

Tue, 12 Sep 2023

**[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen**

Ein entfernter, anonym, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Privilegien zu erweitern.

- [Link](#)

---

Tue, 12 Sep 2023

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

Ein entfernter, anonym 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](#)

---

Tue, 12 Sep 2023

**[UPDATE] [hoch] Notepad++: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Notepad++ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 12 Sep 2023

**[UPDATE] [kritisch] Apple macOS: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Apple macOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

---

Tue, 12 Sep 2023

***[UPDATE] [kritisch] Apple iOS: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 12 Sep 2023

***[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](#)

---

Tue, 12 Sep 2023

***[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung***

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 12 Sep 2023

***[NEU] [hoch] Foxit PDF Editor und Foxit PDF Reader: Mehrere Schwachstellen***

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Foxit PDF Editor und Foxit Reader ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

---

Mon, 11 Sep 2023

***[UPDATE] [hoch] FRRouting Project FRRouting: Mehrere Schwachstellen ermöglichen Denial of Service***

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Mon, 11 Sep 2023

***[UPDATE] [hoch] libssh2: Schwachstelle ermöglicht Denial of Service***

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in libssh2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einzusehen.

- [Link](#)

---

Mon, 11 Sep 2023

***[UPDATE] [hoch] libssh2: Schwachstelle ermöglicht Denial of Service***

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in libssh2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einzusehen.

- [Link](#)

---

Mon, 11 Sep 2023

***[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Mon, 11 Sep 2023

***[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen***

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, Informationen offenzulegen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/12/2023	[Oracle Linux 8 / 9 : cross-gcc (ELSA-2023-28765)]	critical
9/12/2023	[Oracle Linux 8 : cross-gcc (ELSA-2023-28766)]	critical
9/12/2023	[Security Update for Microsoft .NET Core (September 2023)]	high
9/12/2023	[Debian DLA-3562-1 : orthanc - LTS security update]	high
9/12/2023	[RHEL 9 : kernel (RHSA-2023:5069)]	high
9/12/2023	[RHEL 9 : kpatch-patch (RHSA-2023:5093)]	high
9/12/2023	[RHEL 9 : qemu-kvm (RHSA-2023:5094)]	high
9/12/2023	[RHEL 9 : kernel-rt (RHSA-2023:5091)]	high
9/12/2023	[RHEL 9 : dmidecode (RHSA-2023:5061)]	high
9/12/2023	[RHEL 9 : libcap (RHSA-2023:5071)]	high
9/12/2023	[Google Chrome < 117.0.5938.62 Multiple Vulnerabilities]	high
9/12/2023	[Security Updates for Microsoft Word Products (September 2023)]	high
9/12/2023	[Security Updates for Microsoft Visual Studio Products (September 2023)]	high
9/12/2023	[Security Updates for Microsoft SharePoint Server 2016 (September 2023)]	high
9/12/2023	[Security Updates for Microsoft SharePoint Server Subscription Edition (September 2023)]	high
9/12/2023	[Microsoft 3D Viewer app Multiple Remote Code Execution Vulnerabilities (September 2023)]	high
9/12/2023	[Microsoft 3D Builder app Multiple Remote Code Execution Vulnerabilities (September 2023)]	high
9/12/2023	[KB5030261: Windows Server 2008 R2 Security Update (September 2023)]	high
9/12/2023	[KB5030287: Windows Server 2012 R2 Security Update (September 2023)]	high
9/12/2023	[Security Updates for Outlook (September 2023)]	high
9/12/2023	[KB5030286: Windows Server 2008 Security Update (September 2023)]	high
9/12/2023	[KB5030214: Windows 10 version 1809 / Windows Server 2019 Security Update (September 2023)]	high
9/12/2023	[Security Updates for Microsoft Excel Products (September 2023)]	high
9/12/2023	[KB5030325: Windows 2022 / Azure Stack HCI 22H2 Security Update (September 2023)]	high
9/12/2023	[KB5030279: Windows Server 2012 Security Update (September 2023)]	high
9/12/2023	[KB5030211: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (September 2023)]	high
9/12/2023	[KB5030220: Windows 10 LTS 1507 Security Update (September 2023)]	high
9/12/2023	[Security Updates for Microsoft Exchange Server (Sep 2023)]	high
9/12/2023	[Security Updates for Microsoft SharePoint Server 2019 (September 2023)]	high
9/12/2023	[KB5030219: Windows 11 version 22H2 Security Update (September 2023)]	high
9/12/2023	[KB5030213: Windows 10 Version 1607 and Windows Server 2016 Security Update (September 2023)]	high
9/12/2023	[KB5030217: Windows 11 version 21H2 Security Update (September 2023)]	high
9/12/2023	[Microsoft Edge (Chromium) < 116.0.1938.81 (CVE-2023-4863)]	high
9/12/2023	[Ubuntu 22.04 LTS : file vulnerability (USN-6359-1)]	high
9/12/2023	[Ubuntu 20.04 LTS / 22.04 LTS : FLAC vulnerability (USN-6360-1)]	high
9/12/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : RedCloth vulnerability (USN-6358-1)]	high
9/12/2023	[Debian DLA-3564-1 : e2guardian - LTS security update]	high

Datum	Schwachstelle	Bewertung
9/12/2023	[Security Updates for Microsoft Office Products (Sep 2023) (macOS)]	high
9/12/2023	[FreeBSD : zeek – potential DoS vulnerabilities (8eefa87f-31f1-496d-bf8e-2b465b6e4e8a)]	high
9/12/2023	[Oracle Linux 8 : httpd:2.4 (ELSA-2023-5050)]	high



# Aktiv ausgenutzte Sicherheitslücken

## Exploits

“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](#)

---

” “Mon, 11 Sep 2023

### ***Linux 6.4 Use-After-Free***

The Linux 6.4 kernel suffers from a use-after-free condition due to per-VMA locks that introduce a race between page fault and MREMAP\_DONTUNMAP.

- [Link](#)

---

” “Mon, 11 Sep 2023

### ***OpenPLC Webserver 3 Denial Of Service / Buffer Overflow***

A buffer overflow vulnerability in OpenPLC Runtime's webserver version 3 allows attackers to inject malicious code, leading to an internal server error that is irrecoverable. This also disables the ability to add any new slave devices through the "Add Slave Devices" component on the Modbus page of the application.

- [Link](#)

---

" Mon, 11 Sep 2023

### ***Shuttle Booking Software 1.0 SQL Injection***

Shuttle Booking Software version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- [Link](#)

---

" Mon, 11 Sep 2023

### ***Varient News Magazine Script 1.3.0 Insecure Settings***

Varient News Magazine Script version 1.3.0 suffers from an ignored default credential vulnerability.

- [Link](#)

---

" Mon, 11 Sep 2023

### ***IWT Imagine CMS 1.0 Cross Site Scripting***

IWT Imagine CMS version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

" Mon, 11 Sep 2023

### ***iSmile Soft CMS 0.3.0 Cross Site Scripting***

iSmile Soft CMS version 0.3.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

" Fri, 08 Sep 2023

### ***WinRAR Remote Code Execution***

This Metasploit module exploits a vulnerability in WinRAR (CVE-2023-38831). When a user opens a crafted RAR file and its embedded document, the decoy document is executed, leading to code execution.

- [Link](#)

---

" Fri, 08 Sep 2023

### ***LG Simple Editor Remote Code Execution***

This Metasploit module exploits broken access control and directory traversal vulnerabilities in LG Simple Editor software for gaining code execution. The vulnerabilities exist in versions of LG Simple Editor prior to v3.21. By exploiting this flaw, an attacker can upload and execute a malicious JSP payload with the SYSTEM user permissions.

- [Link](#)

---

" Fri, 08 Sep 2023

### ***Sonicwall GMS 9.9.9320 Remote Code Execution***

This Metasploit module exploits a series of vulnerabilities - including auth bypass, SQL injection, and shell injection - to obtain remote code execution on SonicWall GMS versions 9.9.9320 and below.

- [Link](#)

---

" Fri, 08 Sep 2023

### ***OpenTSDB 2.4.1 Unauthenticated Command Injection***

This Metasploit module exploits an unauthenticated command injection vulnerability in the key parameter in OpenTSDB through 2.4.1 in order to achieve unauthenticated remote code execution as the root user. The module first attempts to obtain the OpenTSDB version via the api. If the version is 2.4.1 or lower, the module performs additional checks to obtain the configured metrics and aggregators. It then randomly selects one metric and one aggregator and uses those to instruct the target server to plot a graph. As part of this request, the key parameter is set to the payload, which will then be executed by the target if the latter is vulnerable. This module has been successfully tested against OpenTSDB version 2.4.1.

- [Link](#)

---

" Fri, 08 Sep 2023

### ***Kibana Timelion Prototype Pollution Remote Code Execution***

Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript

code. This leads to an arbitrary command execution with permissions of the Kibana process on the host system. Exploitation will require a service or system reboot to restore normal operation. The WFSDELAY parameter is crucial for this exploit. Setting it too high will cause MANY shells (50-100+), while setting it too low will cause no shells to be obtained. WFSDELAY of 10 for a docker image caused 6 shells.

- [Link](#)

---

” “Fri, 08 Sep 2023

***Microsoft Windows Kernel Recovery Memory Corruption***

The Microsoft Windows Kernel has an issue where a partial success of registry hive log recovery may lead to inconsistent state and memory corruption.

- [Link](#)

---

” “Fri, 08 Sep 2023

***Microsoft Windows Kernel Integer Overflow / Out-Of-Bounds Read***

The Microsoft Windows Kernel suffers from out-of-bounds reads due to an integer overflow in registry .LOG file parsing.

- [Link](#)

---

” “Fri, 08 Sep 2023

***Event Ticketing System 1.0 Cross Site Scripting***

Event Ticketing System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Fri, 08 Sep 2023

***SyncBreeze 15.2.24 Denial Of Service***

SyncBreeze version 15.2.24 suffers from a denial of service vulnerability.

- [Link](#)

---

” “Fri, 08 Sep 2023

***GOM Player 2.3.90.5360 Buffer Overflow***

GOM Player version 2.3.90.5360 suffers from a buffer overflow vulnerability.

- [Link](#)

---

” “Fri, 08 Sep 2023

***Drupal 10.1.2 Web Cache Poisoning***

Drupal version 10.1.2 appears to suffer from web cache poisoning due to a server-side request forgery vulnerability.

- [Link](#)

---

”

## 0-Day

“Tue, 12 Sep 2023

***ZDI-23-1431: Foxit PDF Reader Annotation Use-After-Free Information Disclosure Vulnerability***

- [Link](#)

---

” “Tue, 12 Sep 2023

***ZDI-23-1430: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

---

” “Tue, 12 Sep 2023

***ZDI-23-1429: Foxit PDF Reader PDF File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

---

” “Tue, 12 Sep 2023

***ZDI-23-1428: Foxit PDF Reader AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1427: Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1426: Foxit PDF Reader Annotation Use-After-Free Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1425: Foxit PDF Reader Doc Object Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1424: Foxit PDF Reader XFA Doc Object Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1423: Foxit PDF Reader XFA Doc Object Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1422: Foxit PDF Reader templates Use-After-Free Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1421: Microsoft Office Word FBX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1420: Microsoft Exchange DumpDataReader Deserialization of Untrusted Data Arbitrary File Write Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1419: Microsoft Exchange ApprovedApplicationCollection Deserialization of Untrusted Data Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1418: Microsoft Exchange ProjectInstance Deserialization of Untrusted Data Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1417: Microsoft Exchange Project Deserialization of Untrusted Data Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1416: Microsoft 3D Builder GLB File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1415: Microsoft 3D Builder WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1414: Microsoft 3D Builder PLY File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1413: Microsoft 3D Builder WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1412: Microsoft 3D Builder WRL File Parsing Memory Corruption Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1411: Microsoft 3D Builder PLY File Parsing Memory Corruption Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1410: Microsoft Windows UMPDDrvStrokePath Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1409: Microsoft Windows UMPDDrvStrokeAndFillPath Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1408: Microsoft Windows UMPDDrvStrokeAndFillPath Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1407: Microsoft Windows UMPDDrvBitBlt Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1406: Microsoft Windows UMPDDrvFillPath Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1405: Microsoft Windows CLFS Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1404: Microsoft Windows CLFS Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 12 Sep 2023

*ZDI-23-1403: Microsoft Azure DevOps Server MachinePropertyBag Deserialization of Untrusted Data Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Mon, 11 Sep 2023

*ZDI-23-1402: Hewlett Packard Enterprise OneView resetAdminPassword Authentication Bypass Vulnerability*

- [Link](#)

---

” “Mon, 11 Sep 2023

*ZDI-23-1401: ManageEngine ADManager Plus download Directory Traversal Information Disclosure Vulnerability*

- [Link](#)

---

”

# Die Hacks der Woche

mit Martin Haunschmid

**Private video**

Vorschaubild [Zum Youtube Video](#)

## Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2023-09-11	MGM Resorts	[USA]	<a href="#">Link</a>
2023-09-11	Partenaire de moBiel	[DEU]	<a href="#">Link</a>
2023-09-07	Le groupe hospitalier Saint-Vincent à Strasbourg	[FRA]	<a href="#">Link</a>
2023-09-06	L'académie St Augustine à Maidstone	[GBR]	<a href="#">Link</a>
2023-09-06	Comté de Hinds	[USA]	<a href="#">Link</a>
2023-09-05	Mairie de Séville	[ESP]	<a href="#">Link</a>
2023-09-05	Financial Services Commission (FSC)	[JAM]	<a href="#">Link</a>
2023-09-05	Decatur Independent School District (DISD)	[USA]	<a href="#">Link</a>
2023-09-05	Thermae 2000	[NLD]	<a href="#">Link</a>
2023-09-04	Maiden Erlegh Trust	[GBR]	<a href="#">Link</a>
2023-09-04	Abdelmalek Essaadi University	[MAR]	<a href="#">Link</a>
2023-09-01	Comitato Elettrotecnico Italiano (CEI)	[ITA]	<a href="#">Link</a>
2023-09-01	Secrétariat de l'environnement et des ressources naturelles (Semarnat)	[MEX]	<a href="#">Link</a>



## Ransomware-Erpressungen: (Sep)

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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-08	[PAUL-ALEXANDRE DOICESCO]	qilin	<a href="#">Link</a>
2023-09-08	[WACOAL]	qilin	<a href="#">Link</a>
2023-09-08	[Linktera]	ransomed	<a href="#">Link</a>
2023-09-07	[24/7 Express Logistics ]	ragroup	<a href="#">Link</a>
2023-09-07	[FOCUS Business Solutions]	blackbyte	<a href="#">Link</a>
2023-09-07	[Chambersburg Area School District]	blackbyte	<a href="#">Link</a>
2023-09-07	[Pvc-ms]	stormous	<a href="#">Link</a>
2023-09-07	[toua.net]	lockbit3	<a href="#">Link</a>
2023-09-07	[Conselho Superior da Justiça do Trabalho]	8base	<a href="#">Link</a>
2023-09-07	[Sebata Holdings (MICROmega Holdings)]	bianlian	<a href="#">Link</a>
2023-09-07	[TORMAX USA]	cactus	<a href="#">Link</a>
2023-09-07	[West Craft Manufacturing]	cactus	<a href="#">Link</a>
2023-09-07	[Trimaran Capital Partners]	cactus	<a href="#">Link</a>
2023-09-07	[Specialised Management Services]	cactus	<a href="#">Link</a>
2023-09-06	[nobleweb.com]	lockbit3	<a href="#">Link</a>
2023-09-06	[protosign.it]	lockbit3	<a href="#">Link</a>
2023-09-06	[concrejato.com.br]	lockbit3	<a href="#">Link</a>
2023-09-06	[meroso.be]	lockbit3	<a href="#">Link</a>
2023-09-06	[qsoftnet.com]	lockbit3	<a href="#">Link</a>
2023-09-06	[ragasa.com.mx]	lockbit3	<a href="#">Link</a>
2023-09-06	[I Keating Furniture World]	incransom	<a href="#">Link</a>
2023-09-06	[onyx-fire.com]	lockbit3	<a href="#">Link</a>
2023-09-06	[gormanusa.com]	lockbit3	<a href="#">Link</a>
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	<a href="#">Link</a>
2023-09-06	[It4 Solutions Robras]	incransom	<a href="#">Link</a>
2023-09-06	[Smead]	blackbyte	<a href="#">Link</a>
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	<a href="#">Link</a>
2023-09-06	[Ayass BioScience]	alphv	<a href="#">Link</a>
2023-09-06	[Sabre Corporation]	dunghill_leak	<a href="#">Link</a>
2023-09-06	[Energy One]	akira	<a href="#">Link</a>
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	<a href="#">Link</a>
2023-09-06	[Chula Vista Electric (CVE)]	8base	<a href="#">Link</a>
2023-09-05	[Precisely, Winshuttle]	play	<a href="#">Link</a>
2023-09-05	[Kikkerland Design]	play	<a href="#">Link</a>
2023-09-05	[Markentrainer Werbeagentur]	play	<a href="#">Link</a>
2023-09-05	[Master Interiors]	play	<a href="#">Link</a>
2023-09-05	[Bordelon Marine]	play	<a href="#">Link</a>
2023-09-05	[Majestic Spice]	play	<a href="#">Link</a>
2023-09-04	[Infinity Construction Company]	noescape	<a href="#">Link</a>
2023-09-05	[Maxxd Trailers]	cactus	<a href="#">Link</a>
2023-09-05	[MINEMAN Systems]	cactus	<a href="#">Link</a>
2023-09-05	[Promotrans]	cactus	<a href="#">Link</a>
2023-09-05	[Seymours]	cactus	<a href="#">Link</a>
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	<a href="#">Link</a>
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	<a href="#">Link</a>
2023-09-05	[Marfrig Global Foods]	cactus	<a href="#">Link</a>
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	<a href="#">Link</a>
2023-09-05	[Barry Plant LEAK!]	alphv	<a href="#">Link</a>
2023-09-05	[Barsco]	cactus	<a href="#">Link</a>
2023-09-05	[Foroni SPA]	cactus	<a href="#">Link</a>
2023-09-05	[Hornslyd Købmandsgaard]	cactus	<a href="#">Link</a>
2023-09-05	[Lagarde Meregnani]	cactus	<a href="#">Link</a>
2023-09-05	[spmblaw.com]	lockbit3	<a href="#">Link</a>
2023-09-05	[Unimed]	trigona	<a href="#">Link</a>
2023-09-05	[Cyberport]	trigona	<a href="#">Link</a>
2023-09-05	[godbeylaw.com]	lockbit3	<a href="#">Link</a>
2023-09-01	[Firmdale Hotels]	play	<a href="#">Link</a>
2023-09-04	[easydentalcare.us]	ransomed	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
2023-09-04	[makflix.eu]	ransomed	Link
2023-09-04	[nucleus.live]	ransomed	Link
2023-09-04	[wantager.com]	ransomed	Link
2023-09-04	[Zurvita ]	ragroup	Link
2023-09-04	[Piex Group ]	ragroup	Link
2023-09-04	[Yuxin Automobile Co.Ltd ( )]	ragroup	Link
2023-09-02	[Mulkay Cardiology Consultants]	noescape	Link
2023-09-04	[Balcan]	cactus	Link
2023-09-04	[Barco Uniforms]	cactus	Link
2023-09-04	[Swipe.bg]	ransomed	Link
2023-09-04	[Balmit Bulgaria]	ransomed	Link
2023-09-04	[cdwg.com]	lockbit3	Link
2023-09-04	[Betton France]	medusa	Link
2023-09-04	[Jules B]	medusa	Link
2023-09-04	[VVandA]	8base	Link
2023-09-04	[Prodegest Assessors]	8base	Link
2023-09-04	[Knight Barry Title]	snatch	Link
2023-09-03	[phms.com.au]	ransomed	Link
2023-09-03	[paynesvilleareainsurance.com]	ransomed	Link
2023-09-03	[SKF.com]	ransomed	Link
2023-09-03	[gossilaw.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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-01	[konkconsulting.com]	lockbit3	Link
2023-09-01	[Piex Group]	ragroup	Link
2023-09-01	[Yuxin Automobile Co.Ltd(宇信)]	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](https://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](mailto:info@cyberwald.com)

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