



Ausgabe: 20230915

# 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

### *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](#)

---

### *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](#)

---

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

---

## BSI - Warn- und Informationsdienst (WID)

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, anonym 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](#)

---

Thu, 14 Sep 2023

**[NEU] [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

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

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

- [Link](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] PHP: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Thu, 14 Sep 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um einen Denial of Service Angriff durchzuführen, einen Cross-Site-Scripting-Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

---

Thu, 14 Sep 2023

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

Ein lokaler Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen und um Sicherheitsmechanismen zu umgehen.

- [Link](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] SHA-3 Implementierungen: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in den SHA-3 Implementierungen mehrerer Produkte ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Thu, 14 Sep 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen, um Sicherheitsmechanismen zu umgehen und um unbekannte Auswirkungen zu erzielen.

- [Link](#)

---

Thu, 14 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](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen

Programmcode auszuführen, Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Thu, 14 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](#)

---

Thu, 14 Sep 2023

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

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter anonym Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

---

Thu, 14 Sep 2023

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

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

- [Link](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- [Link](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter anonym Angreifer kann diese Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen und Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

---

Thu, 14 Sep 2023

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

Ein entfernter, anonym, 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](#)

---

Thu, 14 Sep 2023

**[UPDATE] [hoch] Mozilla Firefox: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

---

Datum	Schwachstelle	Bewertung
9/14/2023	[Siemens (CVE-2019-17006)]	critical
9/14/2023	[Siemens (CVE-2021-31895)]	critical
9/14/2023	[AlmaLinux 9 : dmidecode (ALSA-2023:5061)]	high
9/14/2023	[AlmaLinux 9 : kernel-rt (ALSA-2023:5091)]	high
9/14/2023	[AlmaLinux 9 : kpatch-patch (ALSA-2023:5093)]	high
9/14/2023	[AlmaLinux 9 : qemu-kvm (ALSA-2023:5094)]	high
9/14/2023	[Security Updates for Microsoft Team Foundation Server and Azure DevOps Server (September 2023)]	high
9/14/2023	[Debian DSA-5497-1 : libwebp - security update]	high
9/14/2023	[Debian DSA-5496-1 : firefox-esr - security update]	high
9/14/2023	[Slackware Linux 15.0 / current libwebp Vulnerability (SSA:2023-257-01)]	high
9/14/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Mutt vulnerabilities (USN-6374-1)]	high
9/14/2023	[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libssh2 vulnerability (USN-6371-1)]	high
9/14/2023	[Adobe Experience Manager 5.6.1, 6.0.0, and 6.1.0 Multiple Vulnerabilities (APSB16-05)]	high
9/14/2023	[Siemens (CVE-2023-36749)]	high
9/14/2023	[Siemens (CVE-2021-37173)]	high
9/14/2023	[Siemens (CVE-2019-11745)]	high
9/14/2023	[Siemens (CVE-2023-36753)]	high
9/14/2023	[Siemens (CVE-2022-29561)]	high
9/14/2023	[Siemens (CVE-2021-25217)]	high
9/14/2023	[Siemens (CVE-2023-36752)]	high
9/14/2023	[Siemens (CVE-2022-29560)]	high
9/14/2023	[Siemens (CVE-2021-41546)]	high
9/14/2023	[Siemens (CVE-2023-36754)]	high
9/14/2023	[Siemens (CVE-2019-17007)]	high
9/14/2023	[Siemens (CVE-2021-37174)]	high
9/14/2023	[Siemens (CVE-2023-36750)]	high
9/14/2023	[Siemens (CVE-2023-36751)]	high
9/14/2023	[Siemens (CVE-2023-36755)]	high
9/14/2023	[Siemens (CVE-2019-10937)]	high

# Aktiv ausgenutzte Sicherheitslücken

## Exploits

“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](#)

---

” “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](#)

---

”

## 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

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]	<a href="#">Link</a>
2023-09-12	Un prestataire de Pelmorex Corp.	[CAN]	<a href="#">Link</a>
2023-09-12	IFX Networks	[COL]	<a href="#">Link</a>
2023-09-11	MGM Resorts	[USA]	<a href="#">Link</a>
2023-09-11	Partenaire de moBiel	[DEU]	<a href="#">Link</a>
2023-09-11	Le système d'information judiciaire régional (REJIS) du comté de St. Louis	[USA]	<a href="#">Link</a>
2023-09-11	Zetema Progetto Cultura	[ITA]	<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>
2023-09-01	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
2023-09-15	[Steelforce]	trigona	<a href="#">Link</a>
2023-09-14	[wdgroup.com.my]	threeam	<a href="#">Link</a>
2023-09-14	[pvbfabs.com]	threeam	<a href="#">Link</a>
2023-09-14	[intechims.com]	threeam	<a href="#">Link</a>
2023-09-14	[zero-pointorganics.com]	threeam	<a href="#">Link</a>
2023-09-14	[visitingphysiciansnetwork.com]	threeam	<a href="#">Link</a>
2023-09-14	[clearwaterlandscape.com]	threeam	<a href="#">Link</a>
2023-09-14	[Statement on MGM Resorts International: Setting the record straight]	alphv	<a href="#">Link</a>
2023-09-14	[etsi.uy]	knight	<a href="#">Link</a>
2023-09-14	[Ja Quith Press Release]	monti	<a href="#">Link</a>
2023-09-14	[East Baking Press Release]	monti	<a href="#">Link</a>
2023-09-14	[American Steel & Aluminum]	akira	<a href="#">Link</a>
2023-09-14	[Waterford Retirement Residence]	cyphbit	<a href="#">Link</a>
2023-09-14	[Shelly Engineering Metal Work]	cyphbit	<a href="#">Link</a>
2023-09-14	[Harmonic Accounting]	cyphbit	<a href="#">Link</a>
2023-09-14	[Imperador S.R.L.]	cyphbit	<a href="#">Link</a>
2023-09-14	[Waterford Retirement Residence]	cyphbit	<a href="#">Link</a>
2023-09-14	[Shelly Engineering Metal Work]	cyphbit	<a href="#">Link</a>
2023-09-14	[RSV Centrale Bvba]	cyphbit	<a href="#">Link</a>
2023-09-14	[Soprovise]	cyphbit	<a href="#">Link</a>
2023-09-14	[carthagehospital.com]	lockbit3	<a href="#">Link</a>
2023-09-07	[Fondation Vincent De Paul]	noescape	<a href="#">Link</a>
2023-09-07	[EDUCAL, SA de CV]	noescape	<a href="#">Link</a>
2023-09-13	[Enpos]	stormous	<a href="#">Link</a>
2023-09-13	[clearcreek.org]	lockbit3	<a href="#">Link</a>
2023-09-13	[Financial Services Commission]	blacksuit	<a href="#">Link</a>
2023-09-13	[Cedar Holdings]	trigona	<a href="#">Link</a>
2023-09-13	[Benefit Management INC]	knight	<a href="#">Link</a>
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	[Credifel 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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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



Datum	Opfer	Ransomware-Gruppe	Webseite
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	[Hornsyld 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>
2023-09-04	[quantinuum.com]	ransomed	<a href="#">Link</a>
2023-09-04	[laasr.eu]	ransomed	<a href="#">Link</a>
2023-09-04	[medcenter-tambov.ru]	ransomed	<a href="#">Link</a>
2023-09-04	[makflix.eu]	ransomed	<a href="#">Link</a>
2023-09-04	[nucleus.live]	ransomed	<a href="#">Link</a>
2023-09-04	[wantager.com]	ransomed	<a href="#">Link</a>
2023-09-04	[Zurvita ]	ragroup	<a href="#">Link</a>
2023-09-04	[Piex Group ]	ragroup	<a href="#">Link</a>
2023-09-04	[Yuxin Automobile Co.Ltd (  ) ]	ragroup	<a href="#">Link</a>
2023-09-02	[Mulkay Cardiology Consultants]	noescape	<a href="#">Link</a>
2023-09-04	[Balcan]	cactus	<a href="#">Link</a>
2023-09-04	[Barco Uniforms]	cactus	<a href="#">Link</a>
2023-09-04	[Swipe.bg]	ransomed	<a href="#">Link</a>
2023-09-04	[Balmit Bulgaria]	ransomed	<a href="#">Link</a>
2023-09-04	[cdwg.com]	lockbit3	<a href="#">Link</a>
2023-09-04	[Betton France]	medusa	<a href="#">Link</a>
2023-09-04	[Jules B]	medusa	<a href="#">Link</a>
2023-09-04	[VVandA]	8base	<a href="#">Link</a>
2023-09-04	[Prodegest Assessors]	8base	<a href="#">Link</a>
2023-09-04	[Knight Barry Title]	snatch	<a href="#">Link</a>
2023-09-03	[phms.com.au]	ransomed	<a href="#">Link</a>
2023-09-03	[paynesvilleareainsurance.com]	ransomed	<a href="#">Link</a>
2023-09-03	[SKF.com]	ransomed	<a href="#">Link</a>
2023-09-03	[gossilaw.com]	lockbit3	<a href="#">Link</a>
2023-09-03	[marianoshoes.com]	lockbit3	<a href="#">Link</a>
2023-09-03	[Arkopharma]	incransom	<a href="#">Link</a>
2023-09-02	[Taylor University]	moneymessage	<a href="#">Link</a>
2023-09-03	[Riverside Logistics]	moneymessage	<a href="#">Link</a>
2023-09-03	[Estes Design & Manufacturing]	moneymessage	<a href="#">Link</a>
2023-09-03	[Aiphone]	moneymessage	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	ranscoz	Link
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	ranscoz	Link
2023-09-03	[Newton Media A.S]	alphv	<a href="#">Link</a>
2023-09-03	[Lawsonlundell]	alphv	<a href="#">Link</a>
2023-09-02	[glprop.com]	lockbit3	Link
2023-09-02	[Strata Plan Australia]	alphv	<a href="#">Link</a>
2023-09-02	[TissuPath Australia]	alphv	<a href="#">Link</a>
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	<a href="#">Link</a>
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	<a href="#">Link</a>
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	<a href="#">Link</a>
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](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.