



Ausgabe: 20230904

# 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

### *Kritische Lücke in VPN von Securepoint*

Updates sollen eine kritische Sicherheitslücke in der VPN-Software von Securepoint schließen, durch die Angreifer ihre Rechte ausweiten können.

- [Link](#)

---

### *Acronis: Updates dichten Sicherheitslecks in mehreren Produkten ab*

Acronis hat Sicherheitsmeldungen zu insgesamt zwölf Schwachstellen in mehreren Produkten herausgegeben. Updates stehen länger bereit.

- [Link](#)

---

### *VMware Tools: Schwachstelle ermöglicht Angreifern unbefugte Aktionen in Gästen*

VMware warnt vor einer Sicherheitslücke in VMware Tools. Sie ermöglicht eine Man-in-the-Middle-Attacke auf Gastsysteme.

- [Link](#)

---

### *Big Data: Splunk dichtet hochriskante Lücken ab*

Die Big-Data-Experten von Splunk haben aktualisierte Software bereitgestellt, die teils hochriskante Schwachstellen in der Analysesoftware ausbessert.

- [Link](#)

---

### *Sicherheitsupdates: Schadcode-Attacken auf Aruba-Switches möglich*

Verschiedene Switch-Modelle von Aruba sind verwundbar. Abgesicherte Ausgaben von ArubaOS schaffen Abhilfe.

- [Link](#)

---

### *Entwickler von Notepad++ ignoriert offensichtlich Sicherheitslücken*

Mehrere Sicherheitslücken gefährden den Texteditor Notepad++. Trotz Informationen zu den Lücken und möglichen Fixes steht ein Sicherheitsupdate noch aus.

- [Link](#)

---

### *Kritische Sicherheitslücke in VMware Aria Operations for Networks*

VMware schließt Sicherheitslücken in Aria Operations for Networks. Eine gilt als kritisch und erlaubt den Zugriff ohne Anmeldung.

- [Link](#)

---

### *Webbrowser: Google-Chrome-Update stopft hochriskante Sicherheitslücke*

Google bessert im Webbrowser Chrome eine als hochriskant eingestufte Schwachstelle aus.

- [Link](#)

---

### *Webbrowser: Neue Firefox-Releases schließen mehrere Sicherheitslücken*

Die Mozilla-Entwickler haben die Firefox-Versionen 117, ESR 115.2 und ESR 102.15 herausgegeben, die mehrere teils hochriskante Sicherheitslücken schließen.

- [Link](#)

---

### *Zoho ManageEngine: Schwachstelle erlaubt Umgehen von Mehrfaktorauthentifizierung*

In diversen Zoho ManageEngine-Produkten können Angreifer aufgrund einer Sicherheitslücke die Mehrfaktorauthentifizierung umgehen. Updates stehen bereit.

- [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	0.985720000	<a href="#">Link</a>
CVE-2023-38035	0.918170000	0.985360000	<a href="#">Link</a>
CVE-2023-3519	0.911990000	0.984810000	<a href="#">Link</a>
CVE-2023-35078	0.965240000	0.994180000	<a href="#">Link</a>
CVE-2023-34362	0.936790000	0.987800000	<a href="#">Link</a>
CVE-2023-33246	0.963860000	0.993650000	<a href="#">Link</a>
CVE-2023-32315	0.962160000	0.993100000	<a href="#">Link</a>
CVE-2023-28771	0.917110000	0.985250000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987890000	<a href="#">Link</a>
CVE-2023-27372	0.970840000	0.996650000	<a href="#">Link</a>
CVE-2023-27350	0.970860000	0.996670000	<a href="#">Link</a>
CVE-2023-26469	0.910820000	0.984740000	<a href="#">Link</a>
CVE-2023-26360	0.908440000	0.984470000	<a href="#">Link</a>
CVE-2023-25717	0.965660000	0.994400000	<a href="#">Link</a>
CVE-2023-25194	0.924830000	0.986080000	<a href="#">Link</a>
CVE-2023-24489	0.967300000	0.995070000	<a href="#">Link</a>
CVE-2023-21839	0.961720000	0.992950000	<a href="#">Link</a>
CVE-2023-21823	0.907830000	0.984420000	<a href="#">Link</a>
CVE-2023-21554	0.902620000	0.983950000	<a href="#">Link</a>
CVE-2023-20887	0.960660000	0.992660000	<a href="#">Link</a>
CVE-2023-0669	0.965780000	0.994450000	<a href="#">Link</a>

### BSI - Warn- und Informationsdienst (WID)

Fri, 01 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](#)

Fri, 01 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](#)

---

Fri, 01 Sep 2023

***[NEU] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen***

Ein entfernter anonymen Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 01 Sep 2023

***[NEU] [hoch] Moxa MXsecurity: Mehrere Schwachstellen***

Ein Angreifer kann mehrere Schwachstellen in Moxa MXsecurity ausnutzen, um Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 01 Sep 2023

***[NEU] [hoch] Acronis Cyber Protect Home Office: Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen in Acronis Cyber Protect Home Office ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Fri, 01 Sep 2023

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel und Oracle Linux ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Fri, 01 Sep 2023

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

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

- [Link](#)

---

Fri, 01 Sep 2023

***[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen***

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- [Link](#)

---

Fri, 01 Sep 2023

***[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen***

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- [Link](#)

---

Fri, 01 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](#)

---

Fri, 01 Sep 2023

***[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung***

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 01 Sep 2023

***[UPDATE] [hoch] win.rar WinRAR: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in win.rar WinRAR ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 01 Sep 2023

**[UPDATE] [hoch] Juniper JUNOS: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Juniper JUNOS auf Geräten der EX- und SRX Serie ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 01 Sep 2023

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

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

- [Link](#)

---

Fri, 01 Sep 2023

**[UPDATE] [hoch] VMware Aria Operations for Networks: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Networks ausnutzen, um Sicherheitsmaßnahmen zu umgehen und beliebigen Code auszuführen.

- [Link](#)

---

Thu, 31 Aug 2023

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

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

- [Link](#)

---

Thu, 31 Aug 2023

**[NEU] [hoch] IBM AIX: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in IBM AIX und IBM VIOS ausnutzen, um Informationen offenzulegen oder um beliebigen Code auszuführen.

- [Link](#)

---

Thu, 31 Aug 2023

**[NEU] [hoch] Broadcom Brocade SANnav: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Broadcom Brocade SANnav ausnutzen, um Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Thu, 31 Aug 2023

**[NEU] [hoch] HPE Fabric OS: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in HPE Fabric OS ausnutzen, um Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

---

Thu, 31 Aug 2023

**[NEU] [hoch] D-LINK DIR-3040 Router: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann diese Schwachstellen im D-LINK Router ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/3/2023	[Fedora 37 : kernel (2023-a1ca0ef4d6)]	critical
9/3/2023	[Fedora 38 : kernel (2023-da8b7c1ca3)]	critical

Datum	Schwachstelle	Bewertung
9/2/2023	[Fedora 38 : kubernetes (2023-a3fcc0751f)]	critical
9/2/2023	[Fedora 37 : firefox (2023-80549d73b9)]	critical
9/1/2023	[Fedora 38 : firefox (2023-c679c55cf8)]	critical
9/1/2023	[SUSE SLES15 / openSUSE 15 Security Update : php7 (SUSE-SU-2023:3498-1)]	critical
8/31/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : GitPython vulnerability (USN-6326-1)]	critical
9/2/2023	[SUSE SLES15 Security Update : terraform-provider-helm (SUSE-SU-2023:3508-1)]	high
9/1/2023	[Fedora 38 : rust-rustls-webpki (2023-7cb316a73b)]	high
9/1/2023	[Fedora 38 : libeconf (2023-6432bb65ae)]	high
9/1/2023	[Fedora 38 : subscription-manager (2023-29a012c0db)]	high
9/1/2023	[Fedora 37 : rust-rustls-webpki (2023-6ef5f2fbf3)]	high
9/1/2023	[Fedora 37 : subscription-manager (2023-0f2f9bc779)]	high
9/1/2023	[Ubuntu 20.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6331-1)]	high
9/1/2023	[Ubuntu 18.04 ESM : Linux kernel vulnerabilities (USN-6329-1)]	high
9/1/2023	[Ubuntu 20.04 LTS : Linux kernel (GCP) vulnerabilities (USN-6330-1)]	high
9/1/2023	[Ubuntu 23.04 : Linux kernel (Oracle) vulnerabilities (USN-6328-1)]	high
9/1/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6332-1)]	high
9/1/2023	[Ubuntu 16.04 ESM : Linux kernel (KVM) vulnerabilities (USN-6327-1)]	high
9/1/2023	[SUSE SLES12 Security Update : amazon-ssm-agent (SUSE-SU-2023:3501-1)]	high
9/1/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : open-vm-tools (SUSE-SU-2023:3507-1)]	high
9/1/2023	[SUSE SLES12 Security Update : open-vm-tools (SUSE-SU-2023:3506-1)]	high
9/1/2023	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2023-12759)]	high
8/31/2023	[CBL Mariner 2.0 Security Update: haproxy (CVE-2023-40225)]	high
8/31/2023	[Microsoft Edge (Chromium) < 116.0.1938.69 (CVE-2023-4572)]	high
8/31/2023	[RHEL 8 : Red Hat Single Sign-On 7.6.5 security update on RHEL 8 (Important) (RHSA-2023:4919)]	high
8/31/2023	[RHEL 7 : Red Hat Single Sign-On 7.6.5 security update on RHEL 7 (Important) (RHSA-2023:4918)]	high
8/31/2023	[RHEL 9 : Red Hat Single Sign-On 7.6.5 security update on RHEL 9 (Important) (RHSA-2023:4920)]	high
8/31/2023	[FreeBSD : Borg (Backup) – flaw in cryptographic authentication scheme in Borg allowed an attacker to fake archives and indirectly cause backup data loss. (b8a52e5a-483d-11ee-971d-3df00e0f9020)]	high

# Aktiv ausgenutzte Sicherheitslücken

## Exploits

“Sat, 02 Sep 2023

### ***Packet Storm New Exploits For August, 2023***

This archive contains all of the 305 exploits added to Packet Storm in August, 2023.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Tinycontrol LAN Controller 3 Remote Admin Password Change***

Tinycontrol LAN Controller version 3 suffers from an insecure access control allowing an unauthenticated attacker to change accounts passwords and bypass authentication gaining panel control access.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Tinycontrol LAN Controller 3 Remote Credential Extraction***

Tinycontrol LAN Controller version 3 suffers from an issue where an unauthenticated attacker can retrieve the controller’s configuration backup file and extract sensitive information that can allow him/her/them to bypass security controls and penetrate the system in its entirety.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Tinycontrol LAN Controller 3 Denial Of Service***

Tinycontrol LAN Controller version 3 suffers from an unauthenticated remote denial of service vulnerability. An attacker can issue direct requests to the stm.cgi page to reboot and also reset factory settings on the device.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***VMWare Aria Operations For Networks Remote Code Execution***

VMWare Aria Operations for Networks (vRealize Network Insight) static SSH key remote code execution proof of concept exploit.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Microsoft Windows Kernel Use-After-Free***

Microsoft Windows Kernel renaming layered keys does not reference count security descriptors, leading to a use-after-free condition.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Oracle RMAN Missing Auditing***

Proof of concept exploit for Oracle RMAN on Oracle database versions 19c, 18c, 12.2.0.1, and 12.1.0.2 where an RMAN controlfile operation is not adequately logged.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***PlayTube 3.0.1 Information Disclosure***

PlayTube version 3.0.1 suffers from an information leakage vulnerability.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Clcknshop 1.0.0 SQL Injection***

Clcknshop version 1.0.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

---

” “Sat, 02 Sep 2023

### ***Clcknshop 1.0.0 Cross Site Scripting***

Clcknshop version 1.0.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---



” “Thu, 31 Aug 2023

***MsIo64 LOLDriver Memory Corruption***

LOLDriver version 1.3-x64 proof of concept memory corruption exploit.

- [Link](#)

---

” “Thu, 31 Aug 2023

***Easy Address Book Web Server 1.6 Buffer Overflow / Cross Site Scripting***

Easy Address Book Web Server version 1.6 suffers from buffer overflow and cross site scripting vulnerabilities.

- [Link](#)

---

” “Thu, 31 Aug 2023

***PHP JABBERS PHP Review Script 1.0 Cross Site Scripting***

PHP JABBERS PHP Review Script version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Thu, 31 Aug 2023

***Innovins CMS 4.7 SQL Injection***

Innovins CMS version 4.7 suffers from a remote SQL injection vulnerability.

- [Link](#)

---

” “Thu, 31 Aug 2023

***Online ID Generator 1.0 SQL Injection / Shell Upload***

Online ID Generator version 1.0 suffers from remote SQL injection that allows for login bypass and remote shell upload vulnerabilities.

- [Link](#)

---

” “Thu, 31 Aug 2023

***Islam CMS 1.0 Code Injection***

Islam CMS version 1.0 suffers from a remote PHP code injection vulnerability.

- [Link](#)

---

” “Thu, 31 Aug 2023

***Invasor Diagonal CMS 1.0 Cross Site Scripting***

Invasor Diagonal CMS version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Thu, 31 Aug 2023

***InterPhoto 2.3.0 Shell Upload***

InterPhoto version 2.3.0 suffers from a remote shell upload vulnerability.

- [Link](#)

---

” “Wed, 30 Aug 2023

***IQ-Medya CMS 2.0 Cross Site Scripting***

IQ-Medya CMS version 2.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Wed, 30 Aug 2023

***Apache NiFi H2 Connection String Remote Code Execution***

The DBCPConnectionPool and HikariCPConnectionPool Controller Services in Apache NiFi 0.0.2 through 1.21.0 allow an authenticated and authorized user to configure a Database URL with the H2 driver that enables custom code execution. This exploit will result in several shells (5-7). Successfully tested against Apache nifi 1.17.0 through 1.21.0.

- [Link](#)

---

” “Wed, 30 Aug 2023

***Juniper JunOS SRX / EX Remote Code Execution***

A proof of concept exploit for chaining four CVEs to achieve remote code execution in Juniper JunOS within SRX and EX Series products.

- [Link](#)

---

” “Tue, 29 Aug 2023

### *Grawlix 1.5.1 Cross Site Scripting*

Grawlix version 1.5.1 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Tue, 29 Aug 2023

### *GOM Player 2.3.90.5360 MITM / Remote Code Execution*

GOM Player version 2.3.90.5360 man-in-the-middle proof of concept remote code execution exploit.

- [Link](#)

---

” “Tue, 29 Aug 2023

### *ImgHosting 1.2 Cross Site Scripting*

ImgHosting version 1.2 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Tue, 29 Aug 2023

### *imax CMS 1.0 SQL Injection*

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

- [Link](#)

---

”

## 0-Day

“Thu, 31 Aug 2023

### *ZDI-23-1294: Delta Electronics DIAScreen DPA File Parsing Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1293: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1292: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1291: Delta Electronics DOPSoft DPA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1290: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1289: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

### *ZDI-23-1288: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 31 Aug 2023

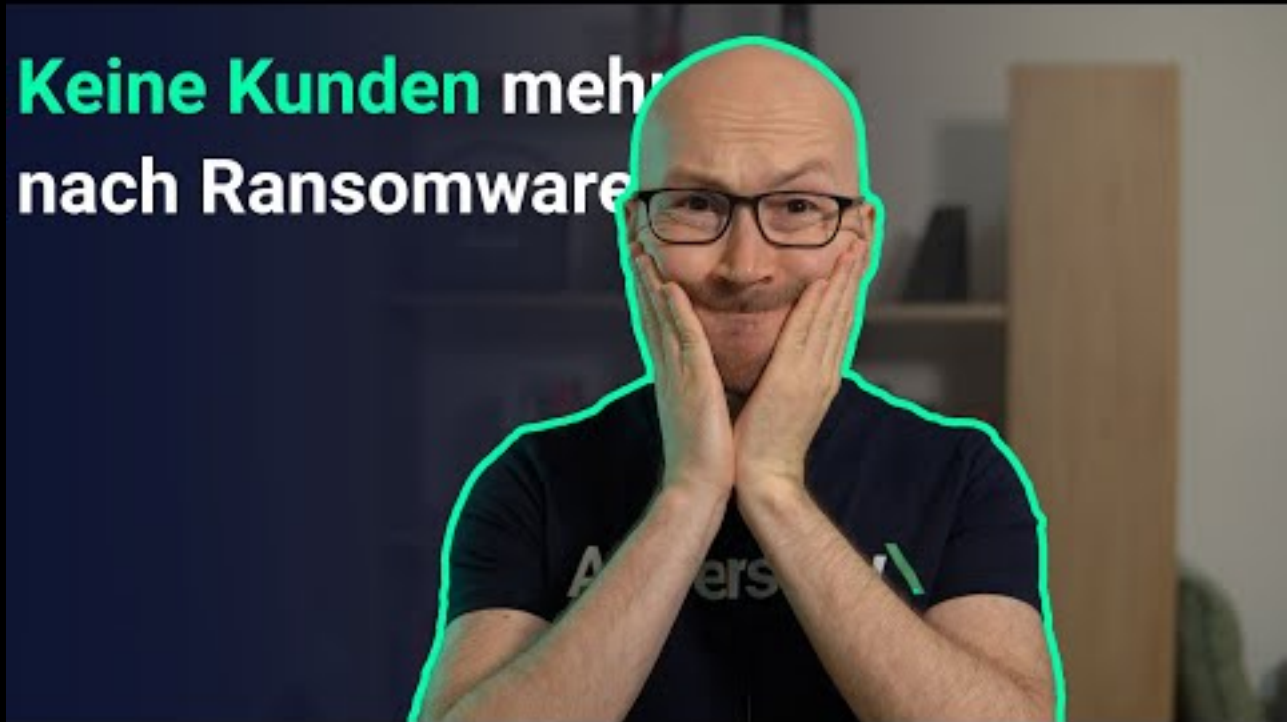
### *ZDI-23-1287: TP-Link Tapo C210 ActiveCells Stack-based Buffer Overflow Remote Code Execution Vulnerability*



## Die Hacks der Woche

mit Martin Haunschmid

“Ich glaube nicht, dass wir danach noch Kunden haben...”



[Zum Youtube Video](#)

## Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
-------	-------	------	-------------

## Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	rancoz	<a href="#">Link</a>
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	rancoz	<a href="#">Link</a>
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	<a href="#">Link</a>
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	<a href="#">Link</a>
2023-09-02	[nerolac.com]	lockbit3	<a href="#">Link</a>
2023-09-02	[ramlowstein.com]	lockbit3	<a href="#">Link</a>
2023-09-02	[Barry Plant Real Estate Australia]	alphv	<a href="#">Link</a>
2023-09-02	[sterncoengineers.com]	lockbit3	<a href="#">Link</a>
2023-09-02	[attorneydanwinder.com]	lockbit3	<a href="#">Link</a>
2023-09-02	[designlink.us]	lockbit3	<a href="#">Link</a>
2023-09-02	[gh2.com]	lockbit3	<a href="#">Link</a>
2023-09-02	[DOIT - Canadian IT company allowed leak of its own clients.]	ragnarlocker	<a href="#">Link</a>
2023-09-02	[SKF.com]	everest	<a href="#">Link</a>
2023-09-02	[Powersportsmarketing.com]	everest	<a href="#">Link</a>
2023-09-02	[Statefarm.com]	everest	<a href="#">Link</a>
2023-09-02	[Aban Tether & OK exchange]	arvinclub	<a href="#">Link</a>
2023-09-02	[cc-gorgesardeche.fr]	lockbit3	<a href="#">Link</a>
2023-09-01	[cciamp.com]	lockbit3	<a href="#">Link</a>
2023-09-01	[Templeman Consulting Group Inc]	bianlian	<a href="#">Link</a>
2023-09-01	[vodatech.com.tr]	lockbit3	<a href="#">Link</a>
2023-09-01	[F??????? ?????s]	play	<a href="#">Link</a>
2023-09-01	[Hawaii Health System]	ransomed	<a href="#">Link</a>
2023-09-01	[hamilton-techservices.com]	lockbit3	<a href="#">Link</a>
2023-09-01	[aquinas.qld.edu.au]	lockbit3	<a href="#">Link</a>
2023-09-01	[konkconsulting.com]	lockbit3	<a href="#">Link</a>
2023-09-01	[Piex Group]	ragroup	<a href="#">Link</a>
2023-09-01	[Yuxin Automobile Co.Ltd( )]	ragroup	<a href="#">Link</a>

# 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.