Cybersecurity Morgenreport

Ausgabe: 20230907

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: 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

—

Webbrowser: Hochriskante Schwachstellen in Google Chrome geschlossen
Google stopft mit aktualisiertern Chrome-Versionen vier als hochriskant eingestufte Sicherheitslücken.
- Link

—

AVM: Fritzbox-Firmware 7.57 und 7.31 stopfen Sicherheitsleck
AVM hat für zahlreiche Fritzboxen die Firmware 7.57 und 7.31 veröffentlicht. Es handelt sich um Stabilitäts- und Sicherheitsupdates.
- Link

—

Jetzt aktualisieren! Proof-of-Concept für kritische VMware-Aria-Lücke
Vergangene Woche hat VMware Updates zum Schließen einer kritischen Sicherheitslücke herausgegeben. Jetzt ist ein Proof-of-Concept verfügbar. Zeit fürs Update!
- Link

—

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

—

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	0.985750000	Link
CVE-2023-38035	0.960130000	0.992550000	Link
CVE-2023-3519	0.911990000	0.984850000	Link
CVE-2023-35078	0.965240000	0.994200000	Link
CVE-2023-34362	0.936790000	0.987840000	Link
CVE-2023-33246	0.963860000	0.993680000	Link
CVE-2023-32315	0.973420000	0.998280000	Link
CVE-2023-28771	0.917110000	0.985290000	Link
CVE-2023-28121	0.937820000	0.987940000	Link
CVE-2023-27372	0.970600000	0.996540000	Link
CVE-2023-27350	0.970860000	0.996690000	Link
CVE-2023-26469	0.910820000	0.984760000	Link
CVE-2023-26360	0.908440000	0.984490000	Link
CVE-2023-25717	0.965660000	0.994430000	Link
CVE-2023-25194	0.924830000	0.986120000	Link
CVE-2023-24489	0.974410000	0.999140000	Link
CVE-2023-21839	0.960800000	0.992730000	Link
CVE-2023-21823	0.907830000	0.984450000	Link
CVE-2023-21554	0.954850000	0.991280000	Link
CVE-2023-20887	0.960660000	0.992690000	Link
CVE-2023-0669	0.965780000	0.994470000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 06 Sep 2023
[NEU] [hoch] Cacti: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

—

Wed, 06 Sep 2023
[NEU] [hoch] Google Android: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erweitern, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen und beliebigen Code auszuführen.

- Link

—

Wed, 06 Sep 2023

[NEU] [hoch] Samsung Android: Mehrere Schwachstellen

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

- Link

—

Wed, 06 Sep 2023

[NEU] [hoch] vim: Schwachstelle ermöglicht Codeausführung, Dos oder Speicheränderung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- Link

—

Wed, 06 Sep 2023

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

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

- Link

—

Wed, 06 Sep 2023

[NEU] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Code auszuführen oder falsche Informationen zu präsentieren.

- Link

—

Wed, 06 Sep 2023

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

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

- Link

—

Wed, 06 Sep 2023

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

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

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] Apache Commons: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Commons ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen, ein Cross-Site-Scritping-Angriff durchzuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] VMware Tanzu Spring Framework: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in VMware Tanzu Spring Framework ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 06 Sep 2023

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

Ein entfernter, anonymer 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

—

Wed, 06 Sep 2023

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

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

- Link

—

Wed, 06 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

—

Wed, 06 Sep 2023

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] vm2: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 06 Sep 2023

[UPDATE] [kritisch] vm2: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 06 Sep 2023

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

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

- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/6/2023	[Debian DLA-3551-1 : otrs2 - LTS security update]	critical
9/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : busybox (SUSE-SU-2023:3529-1)]	critical
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : php7 (SUSE-SU-2023:3528-1)]	critical
9/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gsl (SUSE-SU-2023:3527-1)]	critical
9/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : php7 (SUSE-SU-2023:3541-1)]	critical
9/6/2023	[FreeBSD : chromium – multiple vulnerabilities (df0a2fd1-4c92-11ee-8290-a8a1599412c6)]	critical
9/6/2023	[Debian DLA-3556-1 : aom - LTS security update]	critical
9/6/2023	[Debian DSA-5490-1 : aom - security update]	critical
9/6/2023	[Ubuntu 23.04 : Linux kernel (Azure) vulnerabilities (USN-6344-1)]	critical
9/6/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6350-1)]	critical
9/6/2023	[Amazon Linux 2 : ecs-service-connect-agent (ALASECS-2023-006)]	critical
9/6/2023	[SUSE SLES15 Security Update : container-suseconnect (SUSE-SU-2023:3539-1)]	high
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : buildah (SUSE-SU-2023:3531-1)]	high
9/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : sccache (SUSE-SU-2023:3526-1)]	high
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : kubernetes1.18 (SUSE-SU-2023:3532-1)]	high
9/6/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6342-1)]	high
9/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:3519-1)]	high
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : amazon-ssm-agent (SUSE-SU-2023:3537-1)]	high
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : amazon-ecs-init (SUSE-SU-2023:3522-1)]	high
9/6/2023	[SUSE SLES15 / openSUSE 15 Security Update : docker (SUSE-SU-2023:3536-1)]	high
9/6/2023	[Vim < 9.0.1858]	high
9/6/2023	[Vim < 9.0.1857]	high
9/6/2023	[Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerabilities (USN-6343-1)]	high
9/6/2023	[Juniper Junos OS Vulnerability (JSA72510)]	high
9/6/2023	[AlmaLinux 9 : thunderbird (ALSA-2023:4955)]	high
9/6/2023	[AlmaLinux 9 : firefox (ALSA-2023:4958)]	high
9/6/2023	[AlmaLinux 8 : thunderbird (ALSA-2023:4954)]	high
9/6/2023	[AlmaLinux 8 : firefox (ALSA-2023:4952)]	high
9/6/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6348-1)]	high
9/6/2023	[Ubuntu 20.04 LTS : Linux kernel (Azure CVM) vulnerabilities (USN-6347-1)]	high
9/6/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel (Raspberry Pi) vulnerabilities (USN-6346-1)]	high
9/6/2023	[Ubuntu 20.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6349-1)]	high
9/6/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2023-036)]	high
9/6/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2023-052)]	high
9/6/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2023-039)]	high

Datum	Schwachstelle	Bewertung
9/6/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2023-026)]	high
9/6/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2023-023)]	high
9/6/2023	[Amazon Linux 2 : amazon-ecr-credential-helper (ALASNITRO-ENCLAVES-2023-029)]	high
9/6/2023	[Amazon Linux 2 : amazon-ecr-credential-helper (ALASDOCKER-2023-030)]	high
9/6/2023	[ABB RTU500 Stack-Based Buffer Overflow (CVE-2022-2502)]	high
9/6/2023	[ABB RTU500 Stack-Based Buffer Overflow (CVE-2022-4608)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Wed, 06 Sep 2023
SolarView Compact 6.00 Remote Command Execution
This Metasploit module exploits a command injection vulnerability on the SolarView Compact version 6.00 web application via the vulnerable endpoint downloader.php. After exploitation, an attacker will have full access with the same user privileges under which the webserver is running (typically as user contec).
- Link
—
” “Wed, 06 Sep 2023
WordPress Newsletter 7.8.9 Cross Site Scripting
WordPress Newsletter plugin versions 7.8.9 and below suffer from a persistent cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Microsoft Windows Privilege Escalation
Windows still suffers from issues related to the replacement of the system drive letter during impersonation. This can be abused to trick privilege processes to load configuration files and other resources from untrusted locations leading to elevation of privilege.
- Link
—
” “Wed, 06 Sep 2023
OpenCart CMS 4.0.2.2 Brute Force
OpenCart CMS version 4.0.2.2 suffers from a login brute forcing vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Cleaning Business Software 1.0 Cross Site Scripting
Cleaning Business Software version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Event Booking Calendar 4.0 Cross Site Scripting
Event Booking Calendar version 4.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Firefox 117 Denial Of Service
Firefox version 117 suffers from a file creation denial of service vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Cinema Booking System 1.0 Cross Site Scripting
Cinema Booking System version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
JZDCMS 1.3 Cross Site Scripting
JZDCMS version 1.3 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
Infinity Market Classified Ads Script 1.6.2 Cross Site Scripting
Infinity Market Classified Ads Script version 1.6.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 06 Sep 2023
ImgHosting 1.3 SQL Injection
ImgHosting version 1.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 05 Sep 2023

WordPress Media Library Assistant 3.09 LFI / Remote Code Execution

WordPress Media Library Assistant plugin versions prior to 3.10 are affected by an unauthenticated remote reference to Imagick() conversion which allows attacker to perform local file inclusion and remote code execution depending on the Imagick configuration on the remote server.

- Link

—

” “Tue, 05 Sep 2023

Hikvision Access Control Session Hijacking

Remote attackers can steal valid authentication session identifiers of Hikvision Access Control/Intercom Products. This is possible because a remote attacker can create a session identifier without restrictions. If an attacker requests a session ID at the same time as a valid user, the attacker receives the identical session ID. This session ID is immediately recognized as valid after successful authentication of the correct user.

- Link

—

” “Tue, 05 Sep 2023

Internet Radio auna IR-160 SE UIProto DoS / XSS / Missing Authentication

Internet Radio auna IR-160 SE using the UIProto firmware suffers from missing authentication, cross site scripting, and denial of service vulnerabilities.

- Link

—

” “Tue, 05 Sep 2023

AtlasVPN Linux Client 1.0.3 IP Leak

Remote disconnect exploit for AtlasVPN Linux client version 1.0.3 that will allow a remote website to extract a client’s real IP address.

- Link

—

” “Tue, 05 Sep 2023

Freefloat FTP Server 1.0 Buffer Overflow

Freefloat FTP Server version 1.0 suffers from a remote buffer overflow vulnerability.

- Link

—

” “Tue, 05 Sep 2023

Kingo ROOT 1.5.8 Unquoted Service Path

Kingo ROOT version 1.5.8 suffers from an unquoted service path vulnerability.

- Link

—

” “Tue, 05 Sep 2023

FileMage Gateway 1.10.9 Local File Inclusion

FileMage Gateway version 1.10.9 suffers from a local file inclusion vulnerability.

- Link

—

” “Tue, 05 Sep 2023

WEBIGniter 28.7.23 Shell Upload

WEBIGniter version 28.7.23 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 05 Sep 2023

WEBIGniter 28.7.23 Cross Site Scripting

WEBIGniter version 28.7.23 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 05 Sep 2023

DLINK DPH-400SE FRU2.2.15.8 Information Disclosure

DLINK DPH-400SE version FRU2.2.15.8 suffers from an information disclosure vulnerability.

- Link

—

” “Tue, 05 Sep 2023

WordPress WP Statistics 13.1.5 SQL Injection

WordPress WP Statistics plugin version 13.1.5 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 04 Sep 2023
Linux 6.4 Use-After-Free / Race Condition
There is a race between mbind() and VMA-locked page faults in the Linux 6.4 kernel, leading to a use-after-free condition.
- Link
—
” “Mon, 04 Sep 2023
NVClient 5.0 Stack Buffer Overflow
NVClient version 5.0 suffers from a stack buffer overflow vulnerability.
- Link
—
” “Mon, 04 Sep 2023
CSZ CMS 1.3.0 Cross Site Scripting
CSZ CMS version 1.3.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
”

0-Day

Die Hacks der Woche

mit Martin Haunschmid

NEIN NICHT DIE PAW PATROL & Qakbot Takedown

Zum Youtube Video

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information

Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-06	[nobleweb.com]	lockbit3	Link
2023-09-06	[protosign.it]	lockbit3	Link
2023-09-06	[concrejato.com.br]	lockbit3	Link
2023-09-06	[meroso.be]	lockbit3	Link
2023-09-06	[qsoftnet.com]	lockbit3	Link
2023-09-06	[ragasa.com.mx]	lockbit3	Link
2023-09-06	[I Keating Furniture World]	incransom	Link
2023-09-06	[onyx-fire.com]	lockbit3	Link
2023-09-06	[gormanusa.com]	lockbit3	Link
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	Link
2023-09-06	[It4 Solutions Robras]	incransom	Link
2023-09-06	[Smead]	blackbyte	Link
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	Link
2023-09-06	[Ayass BioScience]	alphv	Link
2023-09-06	[Sabre Corporation]	dunghill_leak	Link
2023-09-06	[Energy One]	akira	Link
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	Link
2023-09-06	[Chula Vista Electric (CVE)]	8base	Link
2023-09-05	[Precisely, Winshuttle]	play	Link
2023-09-05	[Kikkerland Design]	play	Link
2023-09-05	[Markentrainer Werbeagentur]	play	Link
2023-09-05	[Master Interiors]	play	Link
2023-09-05	[Bordelon Marine]	play	Link
2023-09-05	[Majestic Spice]	play	Link
2023-09-04	[Infinity Construction Company]	noescape	Link
2023-09-05	[Maxxd Trailers]	cactus	Link
2023-09-05	[MINEMAN Systems]	cactus	Link
2023-09-05	[Promotrans]	cactus	Link
2023-09-05	[Seymours]	cactus	Link
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	Link
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	Link
2023-09-05	[Marfrig Global Foods]	cactus	Link
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	Link
2023-09-05	[Barry Plant LEAK!]	alphv	Link
2023-09-05	[Barsco]	cactus	Link
2023-09-05	[Foroni SPA]	cactus	Link
2023-09-05	[Hornsyld Købmandsgaard]	cactus	Link
2023-09-05	[Lagarde Meregnani]	cactus	Link
2023-09-05	[spmblaw.com]	lockbit3	Link
2023-09-05	[Unimed]	trigona	Link
2023-09-05	[Cyberport]	trigona	Link
2023-09-05	[godbeylaw.com]	lockbit3	Link
2023-09-01	[Firmdale Hotels]	play	Link
2023-09-04	[easydentalcare.us]	ransomed	Link
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
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

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

Quellen

Quellenverzeichnis

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

Impressum

Herausgeber:
Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail
info@cyberwald.com

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