
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240705



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	11
4 Aktiv ausgenutzte Sicherheitslücken	12
4.1 Exploits der letzten 5 Tage	12
4.2 0-Days der letzten 5 Tage	16
5 Die Hacks der Woche	19
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	19
6 Cyberangriffe: (Jul)	20
7 Ransomware-Erpressungen: (Jul)	20
8 Quellen	22
8.1 Quellenverzeichnis	22
9 Impressum	23

1 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

2 Security-News

2.1 Heise - Security-Alert

Android: Google schließt teils kritische Lücken am Juli-Patchday

Google hat Updates für Android 12, 12L, 13 und 14 im Rahmen des Juli-Patchdays veröffentlicht. Sie schließen Rechteauserweiterungs-Lücken.

- [Link](#)

—

Update für IBM InfoSphere Information Server dichtet viele Sicherheitslücken ab

IBM hat mehrere Sicherheitswarnungen zum InfoSphere Information Server herausgegeben. Aktualisierte Software korrigiert die Fehler.

- [Link](#)

—

Juniper: Notfall-Update für Junos OS auf SRX-Baureihe

Juniper Networks schließt eine als hochriskant eingestufte DoS-Lücke im Juniper OS der SRX-Geräte mit einem Update außer der Reihe.

- [Link](#)

—

RegreSSHion: Sicherheitslücke in OpenSSH gibt geduldigen Angreifern Root-Rechte

Wer die alte, neue Lücke im SSH-Server ausnutzen möchte, braucht Sitzfleisch: Bis zur Root-Shell dauert es 8 Stunden. Dafür klappt der Angriff aus der Ferne.

- [Link](#)

—

IP-Telefonie: Avaya IP Office stopft kritische Sicherheitslecks

Updates für Avaya IP Office dichten Sicherheitslecks in der Software ab. Angreifer können dadurch Schadcode einschleusen.

- [Link](#)

—

Juniper: Kritische Lücke erlaubt Angreifern Übernahme von Session Smart Router

Juniper Networks liefert außerplanmäßige Updates gegen eine kritische Sicherheitslücke in Session Smart Router, -Conductor und WAN Assurance Router.

- [Link](#)

—

APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

- [Link](#)

Bitte patchen! Security-Update behebt kritische Schwachstelle in GitLab

Eine Reihe von Schwachstellen ermöglichen es in GitLab, CI-Pipelines als anderer User zu starten oder Cross-Site-Scripting über Commit Notes einzuschleusen.

- [Link](#)

Google Quickshare: Sicherheitslücke ermöglicht ungefragtes Senden von Dateien

Googles Quickshare, auch als Nearby Share bekannt, kann Angreifern ungefragt Daten an Windows-Rechner schicken lassen.

- [Link](#)

JavaScript-Service Polyfill.io: 100.000 Sites binden Schadcode über CDN ein

Mehrere Sicherheitsforscher melden eine aktive Bedrohung durch das Content Delivery Network von Polyfill.io. Google sperrt Werbung von betroffenen Ads-Seiten.

- [Link](#)

3 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.

3.1 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.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-7028	0.962510000	0.995470000	Link
CVE-2023-6895	0.920390000	0.989640000	Link
CVE-2023-6553	0.934680000	0.991160000	Link
CVE-2023-5360	0.911260000	0.988920000	Link
CVE-2023-52251	0.920390000	0.989650000	Link
CVE-2023-4966	0.971290000	0.998080000	Link
CVE-2023-49103	0.938900000	0.991660000	Link
CVE-2023-48795	0.962520000	0.995470000	Link
CVE-2023-47246	0.953220000	0.993770000	Link
CVE-2023-46805	0.958670000	0.994710000	Link
CVE-2023-46747	0.972100000	0.998380000	Link
CVE-2023-46604	0.963890000	0.995820000	Link
CVE-2023-4542	0.924200000	0.990060000	Link
CVE-2023-43208	0.961280000	0.995200000	Link
CVE-2023-43177	0.959300000	0.994840000	Link
CVE-2023-42793	0.970470000	0.997730000	Link
CVE-2023-41265	0.920320000	0.989630000	Link
CVE-2023-39143	0.940070000	0.991780000	Link
CVE-2023-38646	0.906240000	0.988580000	Link
CVE-2023-38205	0.954590000	0.994020000	Link
CVE-2023-38203	0.968820000	0.997210000	Link
CVE-2023-38146	0.905210000	0.988500000	Link
CVE-2023-38035	0.974610000	0.999610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.965980000	0.996370000	Link
CVE-2023-3519	0.965360000	0.996220000	Link
CVE-2023-35082	0.967060000	0.996680000	Link
CVE-2023-35078	0.968330000	0.997090000	Link
CVE-2023-34993	0.971260000	0.998070000	Link
CVE-2023-34960	0.927460000	0.990360000	Link
CVE-2023-34634	0.927960000	0.990400000	Link
CVE-2023-34468	0.906650000	0.988590000	Link
CVE-2023-34362	0.969920000	0.997560000	Link
CVE-2023-34039	0.945410000	0.992510000	Link
CVE-2023-3368	0.933870000	0.991080000	Link
CVE-2023-33246	0.972570000	0.998580000	Link
CVE-2023-32315	0.973600000	0.999080000	Link
CVE-2023-30625	0.938290000	0.991560000	Link
CVE-2023-30013	0.962250000	0.995390000	Link
CVE-2023-29300	0.969840000	0.997540000	Link
CVE-2023-29298	0.943950000	0.992250000	Link
CVE-2023-28771	0.902140000	0.988330000	Link
CVE-2023-28343	0.948520000	0.993000000	Link
CVE-2023-28121	0.909760000	0.988800000	Link
CVE-2023-27524	0.970570000	0.997760000	Link
CVE-2023-27372	0.973020000	0.998800000	Link
CVE-2023-27350	0.969800000	0.997530000	Link
CVE-2023-26469	0.932230000	0.990900000	Link
CVE-2023-26360	0.957000000	0.994450000	Link
CVE-2023-26035	0.967100000	0.996700000	Link
CVE-2023-25717	0.956860000	0.994420000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.970160000	0.997630000	Link
CVE-2023-2479	0.963760000	0.995790000	Link
CVE-2023-24489	0.973550000	0.999050000	Link
CVE-2023-23752	0.954250000	0.993970000	Link
CVE-2023-23397	0.901800000	0.988300000	Link
CVE-2023-23333	0.963260000	0.995660000	Link
CVE-2023-22527	0.970550000	0.997750000	Link
CVE-2023-22518	0.965950000	0.996360000	Link
CVE-2023-22515	0.973330000	0.998960000	Link
CVE-2023-21839	0.956220000	0.994340000	Link
CVE-2023-21554	0.950840000	0.993340000	Link
CVE-2023-20887	0.971080000	0.997990000	Link
CVE-2023-1671	0.964510000	0.995930000	Link
CVE-2023-0669	0.971300000	0.998090000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 04 Jul 2024

[UPDATE] [hoch] Google Android: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, beliebigen Code zur Ausführung zu bringen und einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] Apple iOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

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

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] LibreOffice: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Thu, 04 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—

Thu, 04 Jul 2024

[UPDATE] [hoch] IBM WebSphere Application Server: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM WebSphere Application Server ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 04 Jul 2024

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

Ein entfernter, anonym oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- [Link](#)

—
Thu, 04 Jul 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 03 Jul 2024

[NEU] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode

Ein lokaler Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- [Link](#)

—

Wed, 03 Jul 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

- [Link](#)

—

Wed, 03 Jul 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 03 Jul 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 03 Jul 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/4/2024	[SUSE SLES12 Security Update : emacs (SUSE-SU-2024:2293-1)]	critical
7/4/2024	[Debian dsa-5725 : znc - security update]	critical
7/4/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Kopano Core vulnerabilities (USN-6876-1)]	critical
7/3/2024	[Slackware Linux 15.0 / current netatalk Multiple Vulnerabilities (SSA:2024-185-01)]	critical
7/4/2024	[Ubuntu 20.04 LTS : Linux kernel (HWE) vulnerabilities (USN-6871-1)]	high
7/4/2024	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-6867-1)]	high
7/4/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libndp (SUSE-SU-2024:2283-1)]	high
7/4/2024	[Fedora 39 : firmitas (2024-139cdfb1fc)]	high
7/4/2024	[Fedora 40 : firmitas (2024-71ef04b872)]	high
7/4/2024	[Fedora 39 : libnbd (2024-3c46dc648c)]	high
7/4/2024	[AlmaLinux 8 : libreoffice (ALSA-2024:4242)]	high
7/4/2024	[AlmaLinux 8 : 389-ds (ALSA-2024:4235)]	high
7/4/2024	[CBL Mariner 2.0 Security Update: glibc (CVE-2023-5156)]	high
7/4/2024	[Ubuntu 24.04 LTS : Linux kernel (Oracle) vulnerabilities (USN-6878-1)]	high

Datum	Schwachstelle	Bewertung
7/4/2024	[Ubuntu 23.10 / 24.04 LTS : LibreOffice vulnerability (USN-6877-1)]	high
7/4/2024	[Oracle Linux 9 : openssh (ELSA-2024-4312)]	high
7/4/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6866-2)]	high
7/3/2024	[Apache Tomcat 9.0.0.M1 < 9.0.90]	high
7/3/2024	[Oracle Linux 9 : glibc (ELSA-2024-12472)]	high
7/3/2024	[Oracle Linux 8 : 389-ds (ELSA-2024-4235)]	high
7/3/2024	[Slackware Linux 15.0 / current httpd Vulnerability (SSA:2024-185-02)]	high
7/3/2024	[Rocky Linux 9 : pki-core (RLSA-2024:4165)]	high
7/3/2024	[Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel vulnerabilities (USN-6865-1)]	high
7/3/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6866-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 04 Jul 2024

Helmholz Industrial Router REX100 / MBConnectline mbNET.mini 2.2.11 Command Injection

Helmholz Industrial Router REX100 and MBConnectline mbNET.mini versions 2.2.11 and below suffer from a command injection vulnerability.

- [Link](#)

—

” “Thu, 04 Jul 2024

Toshiba Multi-Function Printers 40 Vulnerabilities

103 models of Toshiba Multi-Function Printers (MFP) are vulnerable to 40 different vulnerabilities including remote code execution, local privilege escalation, xml injection, and more.

- [Link](#)

—

” “Thu, 04 Jul 2024

Zyxel parse_config.py Command Injection

This Metasploit module exploits vulnerabilities in multiple Zyxel devices including the VPN, USG and APT series. The affected firmware versions depend on the device module, see this module’s documentation for more details.

- [Link](#)

—

” “Thu, 04 Jul 2024

Sharp Multi-Function Printer 18 Vulnerabilities

308 different models of Sharp Multi-Function Printers (MFP) are vulnerable to 18 different vulnerabilities including remote code execution, local file inclusion, credential disclosure, and more.

- [Link](#)

—

” “Thu, 04 Jul 2024

SoftMaker Office / FreeOffice Local Privilege Escalation

SoftMaker Office and FreeOffice suffer from a local privilege escalation vulnerability via the MSI installer. Vulnerable versions include SoftMaker Office 2024 / NX before revision 1214, FreeOffice 2021 Revision 1068, and FreeOffice 2024 before revision 1215.

- [Link](#)

—

” “Thu, 04 Jul 2024

WordPress Photo Gallery 1.8.26 Cross Site Scripting

WordPress Photo Gallery plugin version 1.8.26 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 04 Jul 2024

Siemens CP-8000 / CP-8021 / CP8-022 / CP-8031 / CP-8050 / SICORE Buffer Overread / Escalation

Siemens CP-8000, CP-8021, CP8-022, CP-8031, CP-8050, and SICORE products suffer from buffer overread, privilege escalation, and unsafe storage vulnerabilities.

- [Link](#)

—

” “Wed, 03 Jul 2024

Deep Sea Electronics DSE855 Remote Authentication Bypass

Deep Sea Electronics DSE855 is vulnerable to configuration disclosure when direct object reference is made to the Backup.bin file using an HTTP GET request. This will enable an attacker to disclose sensitive information and help her in authentication bypass, privilege escalation, and full system access.

- [Link](#)

—

” “Tue, 02 Jul 2024

WordPress FooGallery 2.4.16 Cross Site Scripting

WordPress FooGallery plugin version 2.4.16 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 02 Jul 2024

WordPress Gallery 2.3.6 Cross Site Scripting

WordPress Gallery version 2.3.6 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 02 Jul 2024

PowerVR Driver Missing Sanitization

The PowerVR driver does not sanitize ZS-Buffer / MSAA scratch firmware addresses.

- [Link](#)

—

” “Mon, 01 Jul 2024

Packet Storm New Exploits For June, 2024

This archive contains all of the 65 exploits added to Packet Storm in June, 2024.

- [Link](#)

—

” “Mon, 01 Jul 2024

OpenSSH Server regreSSHion Remote Code Execution

Qualys has discovered a a signal handler race condition vulnerability in OpenSSH’s server, sshd. If a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then sshd’s SIGALRM handler is called asynchronously, but this signal handler calls various functions that are not async-signal-safe - for example, syslog(). This race condition affects sshd in its default configuration.

- [Link](#)

—

” “Mon, 01 Jul 2024

Simple Laboratory Management System 1.0 SQL Injection

Simple Laboratory Management System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

Azon Dominator Affiliate Marketing Script SQL Injection

Azon Dominator Affiliate Marketing Script suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

WordPress WPCode Lite 2.1.14 Cross Site Scripting

WordPress WPCode Lite plugin version 2.1.14 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

Xhibiter NFT Marketplace 1.10.2 SQL Injection

Xhibiter NFT Marketplace version 1.10.2 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

Customer Support System 1.0 Cross Site Scripting

Customer Support System version 1.0 suffers from a persistent cross site scripting vulnerability. Original discovery of cross site scripting in this version is attributed to Ahmed Abba in November of 2020.

- [Link](#)

—

” “Thu, 27 Jun 2024

SimpCMS 0.1 Cross Site Scripting

SimpCMS version 0.1 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

Ollama Remote Code Execution

Ollama versions prior to 0.1.34 suffer from a remote code execution vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

SolarWinds Platform 2024.1 SR1 Race Condition

SolarWinds Platform version 2024.1 SR1 suffers from a race condition vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

Automad 2.0.0-alpha.4 Cross Site Scripting

Automad version 2.0.0-alpha.4 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

Poultry Farm Management System 1.0 Shell Upload

Poultry Farm Management System version 1.0 remote shell upload exploit. This is a variant of the original discovery of this flaw in this software version by Hejap Zairy in March of 2022.

- [Link](#)

—

” “Tue, 25 Jun 2024

Faronics WINSelect Hardcoded Credentials / Bad Permissions / Unhashed Password

Faronics WINSelect versions prior to 8.30.xx.903 suffer from having hardcoded credentials, storing unhashed passwords, and configuration file modification vulnerabilities.

- [Link](#)

—

” “Mon, 24 Jun 2024

Netis MW5360 Remote Command Execution

The Netis MW5360 router has a command injection vulnerability via the password parameter on the login page. The vulnerability stems from improper handling of the "password" parameter within the router's web interface. The router's login page authorization can be bypassed by simply deleting the authorization header, leading to the vulnerability. All router firmware versions up to V1.0.1.3442 are vulnerable. Attackers can inject a command in the password parameter, encoded in base64, to exploit the command injection vulnerability. When exploited, this can lead to unauthorized command execution, potentially allowing the attacker to take control of the router.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 03 Jul 2024

ZDI-24-896: Parse Server literalizeRegexPart SQL Injection Authentication Bypass Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-895: Progress Software WhatsUp Gold APM Unrestricted File Upload Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-894: Progress Software WhatsUp Gold CommunityController Unrestricted File Upload Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-893: Progress Software WhatsUp Gold GetFileWithoutZip Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-892: Progress Software WhatsUp Gold WriteDataFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-891: Progress Software WhatsUp Gold OnMessage Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-890: Progress Software WhatsUp Gold SessionControler Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-889: Progress Software WhatsUp Gold InstallController Denial-of-Service Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-888: Progress Software WhatsUp Gold Missing Authentication GetWindowsCredential Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-887: Progress Software WhatsUp Gold GetASPReport Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-886: Progress Software WhatsUp Gold SetAdminPassword Improper Access Control Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-885: Progress Software WhatsUp Gold LoadUsingBasePath Directory Traversal Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 03 Jul 2024

ZDI-24-884: Progress Software WhatsUp Gold LoadCSSUsingBasePath Directory Traversal Information Disclosure Vulnerability

- [Link](#)

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.



[Zum Youtube Video](#)

6 Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link
2024-07-01	Hiap Seng Industries	[SGP]	Link

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link
2024-07-04	[INDA's]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinsa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	Link

8 Quellen

8.1 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>

9 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.