



Ausgabe: 20231009

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

Jetzt patchen! Exploits für glibc-Lücke öffentlich verfügbar

Nachdem der Bug in der Linux-Bibliothek glibc am vergangenen Dienstag bekannt wurde, sind nun zuverlässig funktionierende Exploits aufgetaucht.

- [Link](#)

Sicherheitsupdate: Root-Lücke bedroht Dell SmartFabric Storage Software

Dell hat mehrere gefährliche Sicherheitslücken in SmartFabric Storage Software geschlossen.

- [Link](#)

Malware-Schutz: Watchguard EPDR und AD360 schließen Sicherheitslücken

In den Malware-Schutzlösungen Watchguard EPDR und AD360 klaffen teils Sicherheitslücken mit hohem Risiko. Aktualisierungen stehen bereit.

- [Link](#)

Root- und DoS-Attacken auf Cisco-Produkte möglich

Der Netzwerkausrüster Cisco hat für mehrere Produkte wichtige Sicherheitsupdates veröffentlicht.

- [Link](#)

KI-Tool: Kritische Sicherheitslücken in TorchServe

In TorchServe, einer Komponente des Maschinenlernsystems PyTorch, klaffen kritische Schwachstellen. Updates sollten zügig installiert werden.

- [Link](#)

Sicherheitslücken in Supermicro IPMI: Server übers Internet angreifbar

Kritische Lücken machen Supermicros Überwachungs- und Remote-Control-Funktion IPMI angreifbar. Der Hersteller bietet Updates – aber nur für neuere Boards.

- [Link](#)

Jetzt patchen! Confluence Data Center: Angreifer machen sich zu Admins

Atlassian hat eine kritische Sicherheitslücke in Confluence Data Center und Server geschlossen.

- [Link](#)

Patchday: Attacken auf Android 11, 12 und 13 beobachtet

Unter anderem Google hat wichtige Sicherheitsupdates für Android-Geräte veröffentlicht. Zwei Lücken haben Angreifer bereits im Visier.

- [Link](#)

Webbrowser: Update für Google Chrome schließt Lücke mit hohem Risiko

Google hat dem Webbrowser Chrome ein Sicherheitsupdate spendiert. Es schließt eine Lücke mit hohem Bedrohungsgrad.

- [Link](#)

Angriffe auf ältere Android-Geräte: Lücke in Mali-GPU nur teilweise geschlossen

Aufgrund mehrerer Schwachstellen im Treiber der Grafikeinheit Mali sind unter anderem Smartphone-Modelle von Samsung und Xiaomi verwundbar.

- [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-2023-38035	0.970820000	0.996860000	Link
CVE-2023-35078	0.955330000	0.991670000	Link
CVE-2023-34362	0.920100000	0.985980000	Link
CVE-2023-33246	0.971460000	0.997180000	Link
CVE-2023-32315	0.960720000	0.992970000	Link
CVE-2023-30625	0.932650000	0.987620000	Link
CVE-2023-28771	0.926550000	0.986800000	Link
CVE-2023-27524	0.936870000	0.988200000	Link
CVE-2023-27372	0.971740000	0.997360000	Link
CVE-2023-27350	0.971370000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985800000	Link
CVE-2023-26360	0.915880000	0.985560000	Link
CVE-2023-25717	0.961530000	0.993160000	Link
CVE-2023-25194	0.924830000	0.986560000	Link
CVE-2023-2479	0.963650000	0.993860000	Link
CVE-2023-24489	0.967770000	0.995470000	Link
CVE-2023-21839	0.951010000	0.990640000	Link
CVE-2023-21823	0.929300000	0.987150000	Link
CVE-2023-21554	0.961360000	0.993130000	Link
CVE-2023-20887	0.944590000	0.989420000	Link
CVE-2023-0669	0.967330000	0.995320000	Link

BSI - Warn- und Informationsdienst (WID)

Fri, 06 Oct 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 06 Oct 2023

[NEU] [UNGEPATCHT] [hoch] D-LINK DIR-846 Router: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] poppler: Mehrere Schwachstellen

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] QEMU: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU ausnutzen, um seine Privilegien zu erhöhen, Code auszuführen oder einen Denial of Service zu verursachen.

- [Link](#)

Fri, 06 Oct 2023

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

Ein entfernter, anonymen 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](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Dateien zu manipulieren oder beliebigen Code auszuführen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- [Link](#)

Fri, 06 Oct 2023

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

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Red Hat Quarkus: Schwachstelle ermöglicht die Umgehung von Sicherheitsmaßnahmen oder die Verursachung eines Denial-of-Service-Zustands

Ein entfernter anonym Angreifer kann eine Schwachstelle in Red Hat Quarkus ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Ghostscript: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Drupal: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Drupal ausnutzen, um Informationen offenzulegen.

- [Link](#)

Fri, 06 Oct 2023

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 06 Oct 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/8/2023	[Debian DLA-3601-1 : thunderbird - LTS security update]	critical

Datum	Schwachstelle	Bewertung
10/8/2023	[Debian DLA-3606-1 : freerdp2 - LTS security update]	critical
10/8/2023	[GLSA-202310-06 : Heimdal: Multiple Vulnerabilities]	critical
10/8/2023	[Debian DLA-3610-1 : python-urllib3 - LTS security update]	critical
10/7/2023	[SUSE SLED12 / SLES12 Security Update : python (SUSE-SU-2023:4001-1)]	critical
10/7/2023	[Debian DSA-5519-1 : grub2 - security update]	critical
10/6/2023	[Oracle Linux 8 : firefox (ELSA-2023-5433)]	critical
10/6/2023	[Oracle Linux 8 : thunderbird (ELSA-2023-5428)]	critical
10/6/2023	[Slackware Linux 15.0 / current netatalk Vulnerability (SSA:2023-279-01)]	critical
10/8/2023	[Debian DLA-3607-1 : gnome-boxes - LTS security update]	high
10/8/2023	[Debian DLA-3608-1 : vinagre - LTS security update]	high
10/8/2023	[GLSA-202310-07 : Oracle VirtualBox: Multiple Vulnerabilities]	high
10/8/2023	[GLSA-202310-08 : man-db: privilege escalation]	high
10/8/2023	[Debian DLA-3611-1 : inetutils - LTS security update]	high
10/7/2023	[Oracle Linux 8 : kvm_utils3 (ELSA-2023-12855)]	high
10/7/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : nhttp2 (SUSE-SU-2023:3997-1)]	high
10/7/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : poppler (SUSE-SU-2023:3998-1)]	high
10/7/2023	[Fedora 37 : cups (2023-904f92af98)]	high
10/7/2023	[Fedora 38 : thunderbird (2023-1f5f7b9b92)]	high
10/7/2023	[Fedora 38 : freimage / mingw-freeimage (2023-604a7d56b0)]	high
10/7/2023	[Fedora 38 : vim (2023-b695d3e2a8)]	high
10/6/2023	[Amazon Linux AMI : vim (ALAS-2023-1837)]	high
10/6/2023	[Amazon Linux AMI : poppler (ALAS-2023-1852)]	high
10/6/2023	[Rocky Linux 8 : postgresql:12 (RLSA-2023:4535)]	high
10/6/2023	[Rocky Linux 8 : nodejs:18 (RLSA-2023:4536)]	high
10/6/2023	[Rocky Linux 8 : .NET 7.0 (RLSA-2023:4643)]	high
10/6/2023	[Rocky Linux 8 : postgresql:13 (RLSA-2023:4527)]	high
10/6/2023	[Rocky Linux 8 : thunderbird (RLSA-2023:4954)]	high
10/6/2023	[Rocky Linux 9 : ghostscript (RLSA-2023:5459)]	high
10/6/2023	[Rocky Linux 8 : .NET 6.0 (RLSA-2023:4645)]	high
10/6/2023	[Rocky Linux 8 : firefox (RLSA-2023:4952)]	high
10/6/2023	[Rocky Linux 9 : libeconf (RLSA-2023:4347)]	high
10/6/2023	[Rocky Linux 8 : thunderbird (RLSA-2023:5201)]	high
10/6/2023	[Rocky Linux 8 : glibc (RLSA-2023:5455)]	high
10/6/2023	[Rocky Linux 9 : libwebp (RLSA-2023:5214)]	high
10/6/2023	[Rocky Linux 8 : kernel (RLSA-2023:4517)]	high
10/6/2023	[Oracle Linux 8 : bind9.16 (ELSA-2023-5460)]	high
10/6/2023	[Oracle Linux 9 : ghostscript (ELSA-2023-5459)]	high
10/6/2023	[Oracle Linux 8 : bind (ELSA-2023-5474)]	high
10/6/2023	[Moxa (CVE-2023-4929)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Fri, 06 Oct 2023

glibc ld.so Local Privilege Escalation

Dubbed Looney Tunables, Qualys discovered a buffer overflow vulnerability in the glibc dynamic loader’s processing of the GLIBC_TUNABLES environment variable. This vulnerability was introduced in April 2021 (glibc 2.34) by commit 2ed18c.

- [Link](#)

” “Fri, 06 Oct 2023

SAP Application Server ABAP Open Redirection

SAP Application Server ABAP and ABAP Platform suffer from an open redirection vulnerability.

- [Link](#)

” “Thu, 05 Oct 2023

Chrome ReduceJSLoadPropertyWithEnumeratedKey Out-Of-Bounds Access

Chrome checks in ReduceJSLoadPropertyWithEnumeratedKey are not sufficient to prevent the engine from reading an out-of-bounds index from an enum cache.

- [Link](#)

” “Thu, 05 Oct 2023

Chrome Dangling FixedArray Pointers / Memory Corruption

Chrome suffers from an issue with dangling FixedArray pointers in Torque that can lead to memory corruption.

- [Link](#)

” “Thu, 05 Oct 2023

Chrome SKIA Integer Overflow

When deserializing an SkPath, there is some basic validation performed to ensure that the contents are consistent. This validation does not use safe integer types, or perform additional validation, so it’s possible for a large path to overflow the point count, resulting in an unsafe SkPath object.

- [Link](#)

” “Thu, 05 Oct 2023

edgetpu_pin_user_pages Race Condition

There is a race condition in edgetpu_pin_user_pages which is reachable from some unprivileged contexts, including the Camera app, or the Google Meet app.

- [Link](#)

” “Wed, 04 Oct 2023

Progress Software WS_FTP Unauthenticated Remote Code Execution

This Metasploit module exploits an unsafe .NET deserialization vulnerability to achieve unauthenticated remote code execution against a vulnerable WS_FTP server running the Ad Hoc Transfer module. All versions of WS_FTP Server prior to 2020.0.4 (version 8.7.4) and 2022.0.2 (version 8.8.2) are vulnerable to this issue. The vulnerability was originally discovered by AssetNote.

- [Link](#)

” “Tue, 03 Oct 2023

SAP Enable Now Manager 10.6.5 Build 2804 Cloud Edition CSRF / XSS / Redirect

SAP Enable Now Manager version 10.6.5 Build 2804 Cloud Edition suffers from cross site request forgery, cross site scripting, and open redirection vulnerabilities.

- [Link](#)

” “Tue, 03 Oct 2023

openVIVA c2 20220101 Cross Site Scripting

openVIVA c2 suffers from a persistent cross site scripting vulnerability. Versions prior to 20220801 are affected.

- [Link](#)

” “Tue, 03 Oct 2023

WordPress Contact Form Generator 2.5.5 Cross Site Scripting

WordPress Contact Form Generator plugin version 2.5.5 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Tue, 03 Oct 2023

WordPress KiviCare 3.2.0 Cross Site Scripting

WordPress KiviCard plugin version 3.2.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 02 Oct 2023

Packet Storm New Exploits For September, 2023

This archive contains all of the 122 exploits added to Packet Storm in September, 2023.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter Pre-Auth MPFS Image Remote Code Execution

Electrolink FM/DAB/TV Transmitter allows access to an unprotected endpoint that allows an MPFS File System binary image upload without authentication. The MPFS2 file system module provides a light-weight read-only file system that can be stored in external EEPROM, external serial Flash, or internal Flash program memory. This file system serves as the basis for the HTTP2 web server module, but is also used by the SNMP module and is available to other applications that require basic read-only storage capabilities. This can be exploited to overwrite the flash program memory that holds the web server’s main interfaces and execute arbitrary code.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter Unauthenticated Remote Denial Of Service

Electrolink FM/DAB/TV Transmitter from a denial of service scenario. An unauthenticated attacker can reset the board as well as stop the transmitter operations by sending one GET request to the command.cgi gateway.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter SuperAdmin Hidden Functionality

Electrolink FM/DAB/TV Transmitter allows an unauthenticated attacker to bypass authentication and modify the Cookie to reveal hidden pages that allows more critical operations to the transmitter.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter Vertical Privilege Escalation

Electrolink FM/DAB/TV Transmitter suffers from a privilege escalation vulnerability. An attacker can escalate his privileges by poisoning the Cookie from GUEST to ADMIN to effectively become Administrator or poisoning to ZSL to become Super Administrator.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter Remote Authentication Removal

Electrolink FM/DAB/TV Transmitter suffers from an unauthenticated parameter manipulation that allows an attacker to set the credentials to blank giving her access to the admin panel. It is also vulnerable to account takeover and arbitrary password change.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter (Login Cookie) Authentication Bypass

Electrolink FM/DAB/TV Transmitter suffers from an authentication bypass vulnerability affecting the Login Cookie. An attacker can set an arbitrary value except NO to the Login Cookie and have full system access.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter (controlloLogin.js) Credential Disclosure

Electrolink FM/DAB/TV Transmitter suffers from a disclosure of clear-text credentials in controlloLogin.js that can allow security bypass and system access.

- [Link](#)

” “Mon, 02 Oct 2023

Electrolink FM/DAB/TV Transmitter (login.htm/mail.htm) Credential Disclosure

The Electrolink FM/DAB/TV Transmitter suffers from a disclosure of clear-text credentials in login.htm and mail.htm that can allow security bypass and system access.

- [Link](#)

” “Mon, 02 Oct 2023

Juniper SRX Firewall / EX Switch Remote Code Execution

This Metasploit module exploits a PHP environment variable manipulation vulnerability affecting Juniper SRX firewalls and EX switches. The affected Juniper devices running FreeBSD and every FreeBSD process can access their stdin by opening /dev/fd/0. The exploit also makes use of two useful PHP features. The first being auto_prepend_file which causes the provided file to be added using the require function. The second PHP function is allow_url_include which allows the use of URL-aware fopen wrappers. By enabling allow_url_include, the exploit can use any protocol wrapper with auto_prepend_file. The module then uses data:// to provide a file inline which includes the base64 encoded PHP payload. By default this exploit returns a session confined to a FreeBSD jail with limited functionality. There is a datastore option JAIL_BREAK, that when set to true, will steal the necessary tokens from a user authenticated to the J-Web application, in order to overwrite the root password hash. If there is no user authenticated to the J-Web application this method will not work. The module then authenticates with the new root password over SSH and then rewrites the original root password hash to /etc/master.passwd.

- [Link](#)

” “Fri, 29 Sep 2023

JetBrains TeamCity Unauthenticated Remote Code Execution

This Metasploit module exploits an authentication bypass vulnerability to achieve unauthenticated remote code execution against a vulnerable JetBrains TeamCity server. All versions of TeamCity prior to version 2023.05.4 are vulnerable to this issue. The vulnerability was originally discovered by SonarSource.

- [Link](#)

” “Fri, 29 Sep 2023

Microsoft Windows Kernel Refcount Overflow / Use-After-Free

The Microsoft Windows kernel does not reset security cache during self-healing, leading to refcount overflow and use-after-free conditions.

- [Link](#)

” “Wed, 27 Sep 2023

Microsoft Error Reporting Local Privilege Elevation

This Metasploit module takes advantage of a bug in the way Windows error reporting opens the report parser. If you open a report, Windows uses a relative path to locate the rendering program. By creating a specific alternate directory structure, we can coerce Windows into opening an arbitrary executable as SYSTEM. If the current user is a local admin, the system will attempt impersonation and the exploit will fail.

- [Link](#)

” “Mon, 25 Sep 2023

RoyalTSX 6.0.1 RTSZ File Handling Heap Memory Corruption

RoyalTSX version 6.0.1 suffers from an RTSZ file handling heap memory corruption vulnerability. The application receives SIGABRT after the RAPortCheck.createNWConnection() function is handling the SecureGatewayHost object in the RoyalTSXNativeUI. When the hostname has an array of around 1600 bytes and the Test Connection is clicked the application crashes instantly.

- [Link](#)

”

0-Day

” “Fri, 06 Oct 2023

ZDI-23-1536: Kofax Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 06 Oct 2023

ZDI-23-1535: Microsoft Windows UMPDDrvStretchBlitROP Use-After-Free Local Privilege Escalation Vulnerability

- [Link](#)

” “Fri, 06 Oct 2023

ZDI-23-1534: Microsoft Windows UMPDDrvLineTo Use-After-Free Local Privilege Escalation Vulnerability

- [Link](#)

” “Fri, 06 Oct 2023

ZDI-23-1533: Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1532: Ivanti Endpoint Manager ProcessEPMAuthToken Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1531: Delta Electronics DIAEnergie HandlerUploadCalendar Use Of Hard-Coded Credentials Authentication Bypass Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1530: Delta Electronics DIAEnergie HandlerUploadTag Use Of Hard-Coded Credentials Authentication Bypass Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1529: Delta Electronics DIAEnergie HandlerUploadCarbon Use Of Hard-Coded Credentials Authentication Bypass Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1528: Microsoft PC Manager SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- [Link](#)

” “Thu, 05 Oct 2023

ZDI-23-1527: Microsoft PC Manager SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- [Link](#)

”

Die Hacks der Woche

mit Martin Haunschmid

Good Guy Debugmodus deanonymisiert einen Ransomware-Programmierer | Die webp-Lücke



[Zum Youtube Video](#)

Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-07	Centre hospitalier de l'Ouest Vosgien	[FRA]	Link
2023-10-03	Metro Transit	[USA]	Link
2023-10-02	Estes Express Lines	[USA]	Link
2023-10-02	Hochschule de Karlsruhe	[DEU]	Link
2023-10-02	Provincia di Cosenza	[ITA]	Link
2023-10-02	Degenia	[DEU]	Link
2023-10-02	Le Premier Circuit Judiciaire de Floride	[USA]	Link
2023-10-01	Lyca Mobile UK	[GBR]	Link

Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-09	[BrData Tecnologia]	alphv	Link
2023-10-09	[Southern Arkansas University]	rhysida	Link
2023-10-08	[securicon.co.za]	lockbit3	Link
2023-10-08	[Islamic Azad University of Shiraz]	arvinclub	Link
2023-10-08	[urc-automation.com]	lockbit3	Link
2023-10-08	[IKM]	alphv	Link
2023-10-08	[Petersen Johnson]	8base	Link
2023-10-07	[University Obrany - Part 2 (Tiny Leak)]	monti	Link
2023-10-07	[DallBogg Breach]	ransomed	Link
2023-10-07	[Partnership With Breachforums]	ransomed	Link
2023-10-07	[The Hurley Group]	cactus	Link
2023-10-07	[Healix]	akira	Link
2023-10-06	[International Presence Ltd - Leaked]	ragnarlocker	Link
2023-10-06	[For UNOB]	monti	Link
2023-10-04	[NTT Docomo]	ransomed	Link
2023-10-05	[(SALE) District Of Columbia Elections 600k lines VOTERS DATA]	ransomed	Link
2023-10-06	[Agència Catalana de Notícies (ACN)]	medusa	Link
2023-10-06	[cote-expert-equipements.com]	lockbit3	Link
2023-10-06	[sinedieadvisor.com]	lockbit3	Link
2023-10-06	[tatatelebusiness.com]	lockbit3	Link
2023-10-06	[eemotors.com]	lockbit3	Link
2023-10-06	[bm.co.th]	lockbit3	Link
2023-10-06	[picoft.biz]	lockbit3	Link
2023-10-06	[litung.com.tw]	lockbit3	Link
2023-10-05	[Granger Medical Clinic]	noescape	Link
2023-10-06	[Camara Municipal de Gondomar]	rhysida	Link
2023-10-05	[sirva.com]	lockbit3	Link
2023-10-05	[Low Keng Huat (Singapore) Limited]	bianlian	Link
2023-10-05	[Cornerstone Projects Group]	cactus	Link
2023-10-05	[RICOR Global Limited]	cactus	Link
2023-10-05	[Learning Partnership West - Leaked]	ragnarlocker	Link
2023-10-05	[Terwilliger Land Survey Engineers]	akira	Link
2023-10-04	[DiTRONICS Financial Services]	qilin	Link
2023-10-04	[suncoast-chc.org]	lockbit3	Link
2023-10-04	[Meridian Cooperative]	blackbyte	Link
2023-10-04	[Roof Management]	play	Link
2023-10-04	[Security Instrument]	play	Link
2023-10-04	[Filtration Control]	play	Link
2023-10-04	[Cinepolis USA]	play	Link
2023-10-04	[CHARMANT Group]	play	Link
2023-10-04	[Stavanger Municipality]	play	Link
2023-10-04	[Gruskin Group]	akira	Link
2023-10-04	[McLaren Health Care Corporation]	alphv	Link
2023-10-04	[US Liner Company & American Made LLC]	0mega	Link
2023-10-04	[General Directorate of Migration of the Dominican Republic]	rhysida	Link
2023-10-03	[University of Defence - Part 1]	monti	Link
2023-10-03	[Toscana Promozione]	moneymessage	Link
2023-10-03	[MD LOGISTICS]	moneymessage	Link
2023-10-03	[Maxco Supply]	moneymessage	Link
2023-10-03	[Groupe Fructa Partner - Leaked]	ragnarlocker	Link
2023-10-03	[Somagic]	medusa	Link
2023-10-03	[The One Group]	alphv	Link
2023-10-03	[aicsacorp.com]	lockbit3	Link
2023-10-03	[co.rock.wi.us]	cuba	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-03	[Sabian Inc]	8base	Link
2023-10-03	[Ted Pella Inc.]	8base	Link
2023-10-03	[GDL Logística Integrada S.A]	knight	Link
2023-10-03	[Measuresoft]	mallox	Link
2023-10-02	[RAT.]	donutleaks	Link
2023-10-02	[AllCare Pharmacy]	lorenz	Link
2023-10-02	[Confidential files]	medusalocker	Link
2023-10-02	[Pain Care]	alphv	Link
2023-10-02	[Windak]	medusa	Link
2023-10-02	[Pasouk biological company]	arvinclub	Link
2023-10-02	[Karam Chand Thapar & Bros Coal Sales]	medusa	Link
2023-10-02	[Kirkholm Maskiningeniører]	mallox	Link
2023-10-02	[Federal University of Mato Grosso do Sul]	rhysida	Link
2023-10-01	[erga.com]	lockbit3	Link
2023-10-01	[thermae.nl]	lockbit3	Link
2023-10-01	[ckgroup.com.tw]	lockbit3	Link
2023-10-01	[raeburns.co.uk]	lockbit3	Link
2023-10-01	[tayloredservices.com]	lockbit3	Link
2023-10-01	[fcps1.org]	lockbit3	Link
2023-10-01	[laspesainfamiglia.coop]	lockbit3	Link
2023-10-01	[Cascade Family Dental - Press Release]	monti	Link
2023-10-01	[Rainbow Travel Service - Press Release]	monti	Link
2023-10-01	[Shirin Travel Agency]	arvinclub	Link
2023-10-01	[Flamingo Holland]	trigona	Link
2023-10-01	[Aria Care Partners]	trigona	Link
2023-10-01	[Portesa]	trigona	Link
2023-10-01	[Grupo Boreal]	trigona	Link
2023-10-01	[Quest International]	trigona	Link
2023-10-01	[Arga Medicali]	alphv	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.