Cybersecurity Morgenreport

Ausgabe: 20231003

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! Exploit für kritische Sharepoint-Lücke veröffentlicht
Admins sollten ihre Sharepoint-Server zügig patchen, denn für eine im Juni durch Microsoft behobene Lücke steht jetzt ein Proof-of-Concept-Exploit bereit.
- Link

Angreifer können über Lücken in WS_FTP Daten löschen
Das Softwarepaket für Dateiübertragung WS_FTP ist verwundbar. Die Entwickler haben mehrere Sicherheitslücken geschlossen.
- Link

Kritische Lücke im Mailserver Exim
Der SMTP-Dienst des freien Mailservers Exim enthält eine kritische Schwachstelle, über die Angreifer beliebigen Code ausführen können. Updates sind unterwegs.
- Link

Jetzt patchen! Angreifer haben Netzwerkgeräte von Cisco im Visier
Cisco hat unter anderem eine kritische Lücke in Catalyst SD-WAN geschlossen. Außerdem gibt es Sicherheitsupdates für weitere Produkte.
- Link

Unzählige Anwendungen betroffen: Chaos bei WebP-Lücke
Eine Sicherheitslücke im WebP-Grafikformat betrifft über Googles Chrome hinaus deutlich mehr Anwendungen.
- Link

Zehn Sicherheitslücken in Chrome geschlossen, eine wird bereits ausgenutzt
Google sichert seinen Webbrowser Chrome abermals gegen laufende Attacken ab.
- Link

Schadcode-Lücken in Firefox, Firefox ESR und Thunderbird geschlossen
Mozilla hat seinen Mailclient und seine Webbrowser gegen mögliche Attacken abgesichert.
- Link

Softwareentwicklung: Angreifer können über TeamCity-Lücke Sourcecode stehlen
In einer aktuellen Version von TeamCity haben die Verantwortlichen ein gefährliches Sicherheitsproblem gelöst.
- Link

Sicherheitslücke: Datenleaks auf Drupal-Websites möglich
Unter bestimmten Voraussetzungen können Angreifer mit dem Content Management System Drupal erstellte Seiten attackieren. Abgesicherte Versionen sind verfügbar.
- Link

Qnap warnt vor Codeschmuggel durch Schwachstellen
Qnap warnt vor Sicherheitslücken im QTS-Betriebssystem und der Multimedia Console, durch die Angreifer Schadcode einschleusen können.
- 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	0.996850000	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-2023-28771	0.926550000	0.986790000	Link
CVE-2023-27524	0.936870000	0.988190000	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	0.990630000	Link
CVE-2023-21823	0.907830000	0.984750000	Link
CVE-2023-21554	0.961360000	0.993120000	Link
CVE-2023-20887	0.944590000	0.989410000	Link
CVE-2023-0669	0.967330000	0.995320000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 02 Oct 2023
[UPDATE] [hoch] Google Chrome / Microsoft Edge : Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 02 Oct 2023
[NEU] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Mon, 02 Oct 2023
[NEU] [hoch] Dell NetWorker vProxy: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Dell NetWorker vProxy ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] wpa_supplicant: Schwachstelle ermöglicht Manipulation von Dateien
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in wpa_supplicant und hostapd ausnutzen, um Dateien zu manipulieren.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] libsndfile: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libsndfile ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] ClamAV: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ClamAV ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auf dem System zur Ausführung zu bringen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] binutils: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung
Ein Angreifer kann eine Schwachstelle in libarchive ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.
- Link
—
Mon, 02 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen, Sicherheitsmaßnahmen zu umgehen und Informationen falsch darzustellen.
- Link

—

Mon, 02 Oct 2023

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Mon, 02 Oct 2023

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

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

- Link

—

Mon, 02 Oct 2023

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und andere nicht näher spezifizierte Auswirkungen zu erreichen.

- Link

—

Mon, 02 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

—

Mon, 02 Oct 2023

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 02 Oct 2023

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

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

- Link

—

Mon, 02 Oct 2023

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

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

- Link

—

Mon, 02 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

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/30/2023	[Debian DLA-3590-1 : python-reportlab - LTS security update]	critical
9/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:3898-1)]	critical
9/30/2023	[SUSE SLES15 Security Update : MozillaFirefox (SUSE-SU-2023:3899-1)]	critical
9/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libqb (SUSE-SU-2023:3897-1)]	critical
9/30/2023	[Fedora 37 : firefox (2023-7a4026e363)]	critical
9/30/2023	[Fedora 38 : webkitgtk (2023-e2c2896d16)]	critical
9/30/2023	[Fedora 38 : libwebp (2023-2a0668fe43)]	critical
9/30/2023	[GLSA-202309-16 : wpa_supplicant, hostapd: Multiple Vulnerabilities]	critical
9/30/2023	[GLSA-202309-17 : Chromium, Google Chrome, Microsoft Edge: Multiple Vulnerabilities]	critical
9/30/2023	[Debian DLA-3593-1 : gerbv - LTS security update]	critical
9/30/2023	[Debian DLA-3595-1 : trafficserver - LTS security update]	critical
10/2/2023	[FreeBSD : mediawiki – multiple vulnerabilities (e59fed96-60da-11ee-9102-000c29de725b)]	critical
10/2/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTomMath vulnerability (USN-6402-1)]	critical
10/2/2023	[Debian DSA-5512-1 : exim4 - security update]	critical
10/1/2023	[GLSA-202310-01 : ClamAV: Multiple Vulnerabilities]	critical
9/30/2023	[Debian DSA-5509-1 : firefox-esr - security update]	high
9/30/2023	[Debian DSA-5510-1 : libvpx - security update]	high
9/30/2023	[Debian DSA-5508-1 : chromium - security update]	high
9/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 37 for SLE 15 SP2) (SUSE-SU-2023:3889-1)]	high
9/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 23 for SLE 15 SP3) (SUSE-SU-2023:3892-1)]	high
9/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 39 for SLE 15 SP2) (SUSE-SU-2023:3891-1)]	high
9/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 32 for SLE 15 SP2) (SUSE-SU-2023:3893-1)]	high
9/30/2023	[openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0277-1)]	high
9/30/2023	[GLSA-202309-15 : GNU Binutils: Multiple Vulnerabilities]	high
9/30/2023	[Debian DLA-3591-1 : firefox-esr - LTS security update]	high
9/30/2023	[Slackware Linux 15.0 / current libvpx Vulnerability (SSA:2023-273-01)]	high
9/30/2023	[Slackware Linux 15.0 / current mozilla-thunderbird Vulnerability (SSA:2023-273-02)]	high
9/29/2023	[ABB RTU500 Series Infinite Loop in embedded OpenSSL (CVE-2022-0778)]	high
9/29/2023	[ABB RTU500 Series Type Confusion in embedded OpenSSL (CVE-2023-0286)]	high
10/2/2023	[Fedora 38 : chromium (2023-d66a01ad4f)]	high
10/2/2023	[Debian DLA-3597-1 : open-vm-tools - LTS security update]	high
10/2/2023	[Debian DLA-3598-1 : libvpx - LTS security update]	high
10/2/2023	[Debian DLA-3594-1 : cups - LTS security update]	high
10/2/2023	[Microsoft Edge (Chromium) < 116.0.1938.98 / 117.0.2045.47 Multiple Vulnerabilities]	high
10/2/2023	[Ubuntu 23.04 : libvpx vulnerabilities (USN-6403-1)]	high
10/2/2023	[F5 Networks BIG-IP : Node.js vulnerabilities (K000137093)]	high
10/2/2023	[Fedora 37 : rust-axum / rust-tokio-tungstenite / rust-tungstenite / rust-warp (2023-e72bf7b92e)]	high
10/1/2023	[Debian DLA-3596-1 : firmware-nonfree - LTS security update]	high
10/1/2023	[Fedora 38 : libvpx (2023-c896cf87db)]	high
10/1/2023	[Fedora 37 : chromium (2023-0cd03c3746)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“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
—
” “Mon, 25 Sep 2023
OPNsense 23.1.11_1 / 23.7.3 / 23.7.4 Cross Site Scripting / Privilege Escalation
OPNsense versions 23.1.11_1, 23.7.3, and 23.7.4 suffer from cross site scripting vulnerabilities that can allow for privilege escalation.
- Link
—
” “Mon, 25 Sep 2023
LogoBee CMS 0.2 Cross Site Scripting
LogoBee CMS version 0.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 25 Sep 2023
Lamano LMS 0.1 Insecure Settings

Lamano LMS version 0.1 suffers from an ignored default credential vulnerability.
- Link
—
” “Fri, 22 Sep 2023
Elasticsearch 8.5.3 Stack Overflow
Elasticsearch version 8.5.3 stack overflow proof of concept exploit.
- Link
—
” “Fri, 22 Sep 2023
Taskhub 2.8.8 Cross Site Scripting
Taskhub version 2.8.8 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 21 Sep 2023
TOTOLINK Wireless Routers Remote Command Execution
Multiple TOTOLINK network products contain a command injection vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the command parameter. After exploitation, an attacker will have full access with the same user privileges under which the webserver is running - which is typically root.
- Link
—
” “Thu, 21 Sep 2023
Luxcal Event Calendar 3.2.3 Cross Site Request Forgery
Luxcal Event Calendar version 3.2.3 suffers from a cross site request forgery vulnerability.
- Link
—
” “Wed, 20 Sep 2023
Lamano CMS 2.0 Cross Site Request Forgery
Lamano CMS version 2.0 suffers from a cross site request forgery vulnerability.
- Link
—
” “Wed, 20 Sep 2023
WordPress Theme My Login 2FA Brute Force
WordPress Theme My Login 2FA plugin versions prior to 1.2 suffer from a brute forcing vulnerability.
- Link
—
” “Tue, 19 Sep 2023
Apache Airflow 1.10.10 Remote Code Execution
This Metasploit module exploits an unauthenticated command injection vulnerability by combining two critical vulnerabilities in Apache Airflow version 1.10.10. The first, CVE-2020-11978, is an authenticated command injection vulnerability found in one of Airflow’s example DAGs, ”example_trigger_target_dag”, which allows any authenticated user to run arbitrary OS commands as the user running Airflow Worker/Scheduler. The second, CVE-2020-13927, is a default setting of Airflow 1.10.10 that allows unauthenticated access to Airflow’s Experimental REST API to perform malicious actions such as creating the vulnerable DAG above. The two CVEs taken together allow vulnerable DAG creation and command injection, leading to unauthenticated remote code execution.
- Link
—
” “Tue, 19 Sep 2023
Lexmark Device Embedded Web Server Remote Code Execution
An unauthenticated remote code execution vulnerability exists in the embedded webserver in certain Lexmark devices through 2023-02-19. The vulnerability is only exposed if, when setting up the printer or device, the user selects ”Set up Later” when asked if they would like to add an Admin user. If no Admin user is created, the endpoint /cgi-bin/fax_change_faxtrace_settings is accessible without authentication. The endpoint allows the user to configure a number of different fax settings. A number of the configurable parameters on the page fail to be sanitized properly before being used in a bash eval statement, allowing for an unauthenticated user to run arbitrary commands.
- Link
—
”

0-Day

“Fri, 29 Sep 2023
ZDI-23-1494: Apple Safari TypedArray copyWithin Integer Underflow Remote Code Execution Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1493: G Data Total Security GDBackupSvc Service Link Following Local Privilege Escalation Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1492: Linux Kernel XFRM Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1491: Linux Kernel Netfilter Xtables Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1490: Linux Kernel Netfilter Xtables Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1489: Linux Kernel eBPF Improper Input Validation Privilege Escalation Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1488: ManageEngine ADManager Plus installServiceWithCredentials Command Injection Remote Code Execution Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1487: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1486: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1485: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1484: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1483: PDF-XChange Editor EMF File Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Fri, 29 Sep 2023

ZDI-23-1482: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1481: PDF-XChange Editor JPG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability
- Link
—
” “Fri, 29 Sep 2023
ZDI-23-1480: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure 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

Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
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.