



Ausgabe: 20231004

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

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](#)

Erste Angriffe gesichtet: Angreifer können über Lücken in WS_FTP Daten löschen

Das Softwarepaket für Dateiübertragung WS_FTP ist verwundbar. Die Entwickler haben mehrere Sicherheitslücken geschlossen. Mittlerweile gibt es erste Attacken.

- [Link](#)

Jetzt patchen! Ransomware schlüpft durch kritische TeamCity-Lücke

Angreifer nutzen eine Sicherheitslücke des Software-Distributionssystems TeamCity aus, das weltweit über 30.000 Firmen wie Citibank, HP und Nike einsetzen.

- [Link](#)

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](#)

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](#)

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)

Mon, 02 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](#)

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, anonymmer 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, anonymmer 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, anonymmer 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, anonymmer Angreifer kann eine Schwachstelle in libsndfile ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 02 Oct 2023

[UPDATE] [hoch] ClamAV: Mehrere Schwachstellen

Ein entfernter, anonymmer 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, anonymmer 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, anonymmer 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, anonymmer 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, anonymmer 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, anonym 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, anonym 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, anonym 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 anonym 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, anonym 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
10/3/2023	[Debian DLA-3599-1 : exim4 - LTS security update]	critical
10/3/2023	[Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6404-1)]	critical
10/3/2023	[Ubuntu 20.04 LTS : Thunderbird vulnerabilities (USN-6405-1)]	critical
10/3/2023	[Amazon Linux 2023 : libtommath, libtommath-devel (ALAS2023-2023-370)]	critical
10/3/2023	[Amazon Linux 2023 : ghostscript, ghostscript-gtk, ghostscript-tools-dvipdf (ALAS2023-2023-362)]	critical
10/3/2023	[Slackware Linux 14.0 / 14.1 / 14.2 / 15.0 / current libX11 Multiple Vulnerabilities (SSA:2023-276-01)]	critical
10/3/2023	[Slackware Linux 14.0 / 14.1 / 14.2 / 15.0 / current libXpm Multiple Vulnerabilities (SSA:2023-276-02)]	critical
10/3/2023	[Debian DSA-5513-1 : thunderbird - security update]	critical
10/3/2023	[RHEL 7 : kernel (RHSA-2023:5414)]	high
10/3/2023	[ARM Mali GPU Kernel Driver < r43p0 Improper Memory Access (CVE-2023-4211)]	high
10/3/2023	[Apple TV < 17 Multiple Vulnerabilities (HT213936)]	high
10/3/2023	[GLSA-202310-02 : NVIDIA Drivers: Multiple Vulnerabilities]	high
10/3/2023	[RHEL 7 : kernel (RHSA-2023:5419)]	high
10/3/2023	[GitLab 13.12 < 16.2.8 / 16.3.0 < 16.3.5 / 16.4.0 < 16.4.1 (CVE-2023-5106)]	high
10/3/2023	[Google Chrome < 117.0.5938.149 Vulnerability]	high
10/3/2023	[Google Chrome < 117.0.5938.149 Vulnerability]	high
10/3/2023	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2023-12842)]	high
10/3/2023	[Amazon Linux 2023 : containerd, containerd-stress (ALAS2023-2023-374)]	high
10/3/2023	[Amazon Linux 2023 : aspnetcore-runtime-6.0, aspnetcore-targeting-pack-6.0, dotnet (ALAS2023-2023-369)]	high
10/3/2023	[Amazon Linux 2023 : cups, cups-client, cups-devel (ALAS2023-2023-361)]	high
10/3/2023	[Amazon Linux 2023 : libwebp, libwebp-devel, libwebp-java (ALAS2023-2023-358)]	high
10/3/2023	[Amazon Linux 2023 : bind, bind-chroot, bind-devel (ALAS2023-2023-372)]	high
10/3/2023	[Amazon Linux 2023 : libwebp, libwebp-devel, libwebp-java (ALAS2023-2023-355)]	high
10/3/2023	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2023-356)]	high
10/3/2023	[Amazon Linux 2023 : pmix, pmix-devel, pmix-pmi (ALAS2023-2023-363)]	high
10/3/2023	[Amazon Linux 2023 : curl, curl-minimal, libcurl (ALAS2023-2023-368)]	high
10/3/2023	[Amazon Linux 2023 : vim-common, vim-data, vim-default-editor (ALAS2023-2023-360)]	high
10/3/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6386-3)]	high
10/3/2023	[Debian DLA-3600-1 : postgresql-11 - LTS security update]	high
10/3/2023	[Sprecher Automation SPRECON-E TCP SACK PANIC (CVE-2019-11477)]	high
10/3/2023	[Sprecher Automation SPRECON-E TCP SACK PANIC (CVE-2019-11479)]	high
10/3/2023	[Sprecher Automation SPRECON-E TCP SACK PANIC (CVE-2019-11478)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“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](#)

” “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](#)

”

0-Day

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
2023-10-02	Estes Express Lines	[USA]	Link

Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-04	[US Liner Company & American Made LLC]	Omega	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
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.