Cybersecurity Morgenreport

Ausgabe: 20231002

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

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

—

Sicherheitsupdate: Authentifizierung von HPE OneView umgehbar
Die IT-Infrastrukturmanagementlösung OneView von HPE ist verwundbar. Der Entwickler hat zwei kritische Sicherheitslücken geschlossen.
- Link

—

Sicherheitsupdate: Passwort-Lücke bedroht Nagios XI
Angreifer können die Server-Monitoring-Lösung Nagios XI attackieren. Eine dagegen abgesicherte Version ist verfügbar.
- 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	0.991660000	Link
CVE-2023-34362	0.920100000	0.985970000	Link
CVE-2023-33246	0.971460000	0.997180000	Link
CVE-2023-32315	0.960720000	0.992970000	Link
CVE-2023-28771	0.926550000	0.986780000	Link
CVE-2023-27524	0.936870000	0.988190000	Link
CVE-2023-27372	0.971740000	0.997350000	Link
CVE-2023-27350	0.971370000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985790000	Link
CVE-2023-26360	0.915880000	0.985560000	Link
CVE-2023-25717	0.958870000	0.992490000	Link
CVE-2023-25194	0.924830000	0.986540000	Link
CVE-2023-2479	0.963650000	0.993850000	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	0.989420000	Link
CVE-2023-0669	0.967330000	0.995320000	Link

BSI - Warn- und Informationsdienst (WID)

Fri, 29 Sep 2023
[NEU] [hoch] GitLab: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um beliebigen Programmcode mit Rechten des Benutzers auszuführen, Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen oder Dateien zu manipulieren.
- Link

Fri, 29 Sep 2023
[NEU] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 29 Sep 2023

[NEU] [hoch] Mozilla Firefox: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 29 Sep 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

—

Fri, 29 Sep 2023

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 29 Sep 2023

[UPDATE] [kritisch] Red Hat JBoss Enterprise Application Platform: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Fri, 29 Sep 2023

[UPDATE] [hoch] Juniper JUNOS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Juniper JUNOS auf Geräten der EX- und SRX Serie ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 29 Sep 2023

[UPDATE] [hoch] OPNsense: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in OPNsense ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- Link

—

Fri, 29 Sep 2023

[UPDATE] [kritisch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen preiszugeben, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Thu, 28 Sep 2023

[NEU] [hoch] Cisco IOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco IOS und Cisco IOS XE ausnutzen, um seine Rechte zu erweitern, einen Denial of Service zu verursachen, Dateien zu manipulieren oder Informationen offenzulegen.

- Link

—

Thu, 28 Sep 2023

[NEU] [UNGEPATCHT] [hoch] Cisco IOS XE: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Cisco IOS XE ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- Link

—

Thu, 28 Sep 2023

[NEU] [hoch] Cisco Catalyst SD-WAN: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco Catalyst ausnutzen, um Informationen offenzulegen,

Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen und Daten zu manipulieren.
- Link

—

Thu, 28 Sep 2023
[NEU] [hoch] Progress Software WS_FTP: Mehre Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Progress Software WS_FTP ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting und Cross-Site Request Forgery Angriffe durchzuführen.
- Link

—

Thu, 28 Sep 2023
[NEU] [UNGEPATCHT] [kritisch] Exim: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Exim ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.
- Link

—

Thu, 28 Sep 2023
[NEU] [hoch] Cisco Digital Network Architecture Center: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Cisco Digital Network Architecture Center ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Thu, 28 Sep 2023
[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 28 Sep 2023
[NEU] [UNGEPATCHT] [hoch] Avast Premium Security: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in Avast Premium Security ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.
- Link

—

Thu, 28 Sep 2023
[NEU] [hoch] Dell NetWorker: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
Ein Angreifer kann eine Schwachstelle in Dell NetWorker ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen und Daten zu manipulieren.
- Link

—

Thu, 28 Sep 2023
[UPDATE] [hoch] Nginx: Schwachstelle ermöglicht Privilegieneskalation
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Debian Linux Jessie (8.0) und Ubuntu Linux ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Thu, 28 Sep 2023
[UPDATE] [hoch] Ruby: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Daten zu manipulieren, vertrauliche Daten einzusehen oder einen Denial of Service Angriff durchzuführen.
- 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	[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
9/29/2023	[Debian DLA-3587-1 : firefox-esr - LTS security update]	critical
9/29/2023	[GLSA-202309-14 : libarchive: Multiple Vulnerabilities]	critical
9/29/2023	[CBL Mariner 2.0 Security Update: libtommath / tcl (CVE-2023-36328)]	critical
9/29/2023	[ABB RTU500 Series Buffer Overflow in embedded OpenSSL (CVE-2021-3711)]	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	[Fedora 38 : libwebp (2023-2a0668fe43)]	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	[Debian DLA-3588-1 : vim - LTS security update]	high
9/29/2023	[Ubuntu 22.04 LTS : Linux kernel (Raspberry Pi) vulnerabilities (USN-6386-2)]	high
9/29/2023	[ABB RTU500 Series Out-of-bounds Read in embedded VxWorks (CVE-2022-23937)]	high
9/29/2023	[ABB RTU500 Series Out-of-bounds Read in embedded OpenSSL (CVE-2021-3712)]	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
10/1/2023	[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

“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
—
” “Tue, 19 Sep 2023
WordPress Essential Blocks 4.2.0 / Essential Blocks Pro 1.1.0 PHP Object Injection
WordPress Essential Blocks plugin versions 4.2.0 and below and Essential Blocks Pro versions 1.1.0 and below suffer from multiple PHP object injection vulnerabilities.
- Link
—
” “Tue, 19 Sep 2023
Taskhub 2.8.7 SQL Injection
Taskhub version 2.8.7 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 19 Sep 2023
Packers And Movers Management System 1.0 SQL Injection
Packers and Movers Management System version 1.0 suffers from a remote blind SQL injection vulnerability. Proof of concept exploit written in python included.
- Link
—

” “Tue, 19 Sep 2023
Super Store Finder 3.7 Remote Command Execution
Super Store Finder versions 3.7 and below suffer from a remote command execution vulnerability.
- Link
—
” “Tue, 19 Sep 2023
Lamano CMS 2.0 SQL Injection
Lamano CMS version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Tue, 19 Sep 2023
Lacabane 1.0 SQL Injection
Lacabane version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Tue, 19 Sep 2023
Free And Open Source Inventory Management System 1.0 SQL Injection
Free and Open Source Inventory Management System version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 18 Sep 2023
Atos Unify OpenScape Code Execution / Missing Authentication
Atos Unify OpenScape Session Border Controller, Atos Unify OpenScape Branch, and Atos Unify OpenScape BCF suffer from remote code execution and missing authentication vulnerabilities. Atos OpenScape SBC versions before 10 R3.3.0, Branch version 10 versions before R3.3.0, and BCF version 10 versions before 10 R10.10.0 are affected.
- Link
—
” “Mon, 18 Sep 2023
PTC - Codebeamer Cross Site Scripting
PTC - Codebeamer versions 22.10-SP7 and below, 22.04-SP5 and below, and 21.09-SP13 and below suffer from a cross site scripting vulnerability.
- Link
—
” “Mon, 18 Sep 2023
Ivanti Avalanche MDM Buffer Overflow
This Metasploit module exploits a buffer overflow condition in Ivanti Avalanche MDM versions prior to 6.4.1. An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in arbitrary code execution with the NT/AUTHORITY SYSTEM permissions. This vulnerability occurs during the processing of 3/5/8/100/101/102 item data types. The program tries to copy the item data using qmemcopy to a fixed size data buffer on stack. Upon successful exploitation the attacker gains full access to the target system. This vulnerability has been tested against Ivanti Avalanche MDM version 6.4.0.0 on Windows 10.
- 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
2023-10-02	[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.