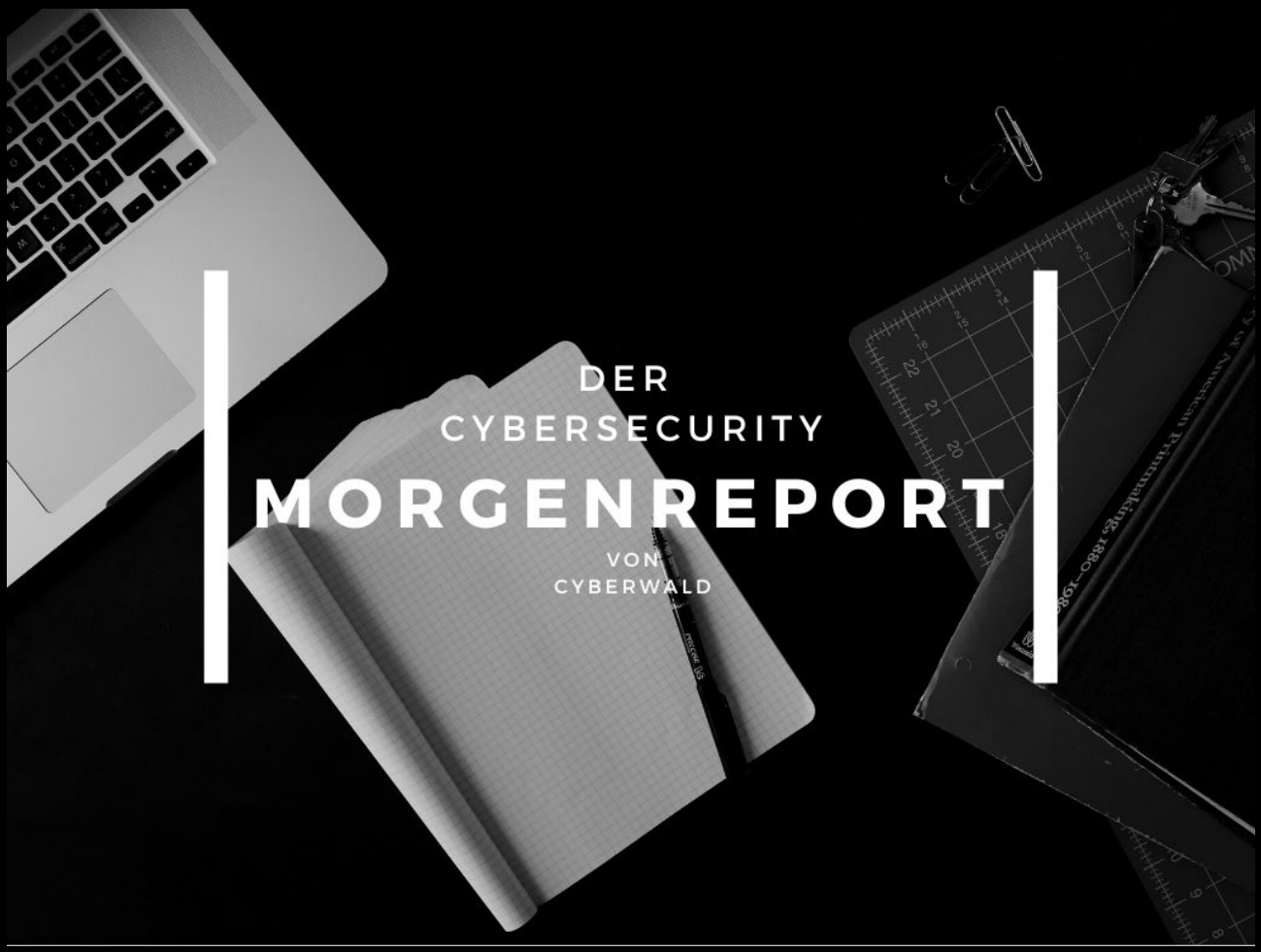
Cybersecurity Morgenreport



Ausgabe: 20231011

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

Patchday Microsoft: Attacken auf Skype for Business und WordPad
Microsoft hat wichtige Sicherheitsupdates für etwa Azure, Office und Windows veröffentlicht.
- Link

—

libcue-Lücke reißt Sicherheitsleck in Gnome
Eine Schwachstelle in einer unscheinbaren Bibliothek führt zu einer veritablen Sicherheitslücke in Gnome. Updates stehen bereit.
- Link

—

Sicherheitsupdates: Schadcode- und Root-Lücken bedrohen IBM-Software
IBM hat unter anderem im Datenbankmanagementsystem Db2 schwerwiegende Schwachstellen geschlossen.
- Link

—

Backup: Acronis schließt Sicherheitslücken im Agent für Linux, Mac und Windows
Acronis hat eine Aktualisierung des Agent für Linux, Mac und Windows veröffentlicht. Sie dichtet unter anderem ein Leck mit hohem Risiko ab.
- Link

—

SAP: Patchday im Oktober geht ruhiger zu
Der Patchday von SAP im Oktober bringt lediglich sieben Benachrichtigungen zu Schwachstellen. Der Hersteller stuft deren Risiko als mittel ein.
- Link

—

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

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-2023-42793	0.972090000	0.997570000	Link
CVE-2023-38035	0.970820000	0.996860000	Link
CVE-2023-35078	0.959430000	0.992630000	Link
CVE-2023-34362	0.921790000	0.986210000	Link
CVE-2023-33246	0.971460000	0.997190000	Link
CVE-2023-32315	0.960720000	0.992980000	Link
CVE-2023-30625	0.932650000	0.987690000	Link
CVE-2023-30013	0.936180000	0.988140000	Link
CVE-2023-28771	0.926550000	0.986820000	Link
CVE-2023-27524	0.932860000	0.987750000	Link
CVE-2023-27372	0.971800000	0.997420000	Link
CVE-2023-27350	0.971370000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985810000	Link
CVE-2023-26360	0.919780000	0.986000000	Link
CVE-2023-25717	0.961530000	0.993160000	Link
CVE-2023-25194	0.924830000	0.986590000	Link
CVE-2023-2479	0.964610000	0.994190000	Link
CVE-2023-24489	0.967770000	0.995490000	Link
CVE-2023-21839	0.951010000	0.990670000	Link
CVE-2023-21823	0.929300000	0.987220000	Link
CVE-2023-21554	0.961360000	0.993130000	Link
CVE-2023-20887	0.932820000	0.987730000	Link
CVE-2023-0669	0.968230000	0.995640000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 10 Oct 2023
[NEU] [hoch] F5 BIG-IP: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in F5 BIG-IP ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Tue, 10 Oct 2023
[NEU] [hoch] GNOME: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GNOME ausnutzen, um beliebigen Programmcode auszuführen.
- Link

Tue, 10 Oct 2023
[NEU] [hoch] Siemens SICAM: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Siemens SICAM ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.
- Link

Tue, 10 Oct 2023
[NEU] [hoch] SAP Patchday Oktober 2023
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Daten zu manipulieren und einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

Tue, 10 Oct 2023
[UPDATE] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um seine Privilegien zu erhöhen, Daten zu manipulieren oder offenzulegen, Sicherheitsvorkehrungen zu umgehen, oder einen Denial of Service zu verursachen.
- Link

Tue, 10 Oct 2023
[UPDATE] [hoch] Node.js: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.
- Link

Tue, 10 Oct 2023
[UPDATE] [hoch] Cacti: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

Tue, 10 Oct 2023
[UPDATE] [kritisch] JetBrains TeamCity: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in JetBrains TeamCity ausnutzen, um beliebigen Programmcode auszuführen, administrative Rechte zu erlangen oder einen Cross Site Scripting Angriff durchzuführen.
- Link

Tue, 10 Oct 2023
[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen oder seine Privilegien zu erweitern.
- Link

Tue, 10 Oct 2023
[NEU] [hoch] Red Hat Enterprise Linux (libvpx): Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Komponente libvpx ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.
- Link

Mon, 09 Oct 2023
[NEU] [hoch] MediaWiki: Mehre Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in MediaWiki ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Cross-Site-Scripting-Angriffe

durchzuführen oder vertrauliche Informationen offenzulegen.
- Link
—
Mon, 09 Oct 2023
[NEU] [hoch] IBM DB2: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Manipulation
Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um HTTP Anfragen zu manipulieren.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herzustellen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Dateien zu manipulieren.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen und einen Denial of Service Zustand zu verursachen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] Intel BIOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein lokaler Angreifer kann mehrere Schwachstellen im Intel BIOS ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Mon, 09 Oct 2023
[UPDATE] [hoch] Heimdal: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Heimdal, Samba, MIT Kerberos und FreeBSD Project FreeBSD OS ausnutzen, um einen Denial of Service Angriff durchzuführen, und um beliebigen Code auszuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/10/2023	[RHEL 7 : python-reportlab (RHSA-2023:5616)]	critical
10/10/2023	[RHEL 9 : libqb (RHSA-2023:5597)]	critical
10/10/2023	[Ubuntu 22.04 LTS / 23.04 : WebKitGTK vulnerabilities (USN-6426-1)]	critical
10/10/2023	[Google Chrome < 118.0.5993.70 Multiple Vulnerabilities]	critical
10/10/2023	[Google Chrome < 118.0.5993.70 Multiple Vulnerabilities]	critical
10/10/2023	[KB5031364: Windows 2022 / Azure Stack HCI 22H2 Security Update (October 2023)]	critical
10/10/2023	[KB5031377: Windows 10 LTS 1507 Security Update (October 2023)]	critical
10/10/2023	[KB5031411: Windows Server 2008 Security Update (October 2023)]	critical
10/10/2023	[KB5031356: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (October 2023)]	critical
10/10/2023	[KB5031354: Windows 11 version 22H2 Security Update (October 2023)]	critical
10/10/2023	[KB5031427: Windows Server 2012 Security Update (October 2023)]	critical
10/10/2023	[KB5031441: Windows Server 2008 R2 Security Update (October 2023)]	critical
10/10/2023	[KB5031358: Windows 11 version 21H2 Security Update (October 2023)]	critical
10/10/2023	[KB5031362: Windows 10 Version 1607 and Windows Server 2016 Security Update (October 2023)]	critical
10/10/2023	[KB5031407: Windows Server 2012 R2 Security Update (October 2023)]	critical
10/10/2023	[KB5031361: Windows 10 version 1809 / Windows Server 2019 Security Update (October 2023)]	critical
10/10/2023	[Debian DSA-5520-1 : mediawiki - security update]	critical
10/10/2023	[Oracle Linux 7 : python-reportlab (ELSA-2023-5616)]	critical
10/10/2023	[RHEL 8 : kernel-rt (RHSA-2023:5588)]	high
10/10/2023	[RHEL 7 : kernel (RHSA-2023:5622)]	high
10/10/2023	[RHEL 8 : kernel (RHSA-2023:5627)]	high
10/10/2023	[RHEL 8 : kpatch-patch (RHSA-2023:5548)]	high
10/10/2023	[RHEL 7 : libssh2 (RHSA-2023:5615)]	high
10/10/2023	[RHEL 9 : kpatch-patch (RHSA-2023:5575)]	high
10/10/2023	[RHEL 8 : kpatch-patch (RHSA-2023:5580)]	high
10/10/2023	[RHEL 9 : kernel (RHSA-2023:5604)]	high
10/10/2023	[RHEL 7 : kpatch-patch (RHSA-2023:5574)]	high
10/10/2023	[RHEL 8 : kernel (RHSA-2023:5628)]	high
10/10/2023	[RHEL 8 : kernel (RHSA-2023:5589)]	high
10/10/2023	[RHEL 9 : kernel-rt (RHSA-2023:5603)]	high
10/10/2023	[Security Updates for Microsoft Office Products (Oct 2023) (macOS)]	high
10/10/2023	[Oracle Linux 9 : glibc (ELSA-2023-5453)]	high
10/10/2023	[Oracle Linux 8 : glibc (ELSA-2023-5455)]	high
10/10/2023	[Security Updates for Microsoft Exchange Server (Oct 2023)]	high
10/10/2023	[Security Updates for Microsoft Skype for Business (October 2023)]	high
10/10/2023	[Security Updates for Microsoft Team Foundation Server and Azure DevOps Server (October 2023)]	high
10/10/2023	[Microsoft Azure RTOS GUIX Studio Multiple Vulnerabilities (October 2023)]	high
10/10/2023	[Oracle Linux 7 : libssh2 (ELSA-2023-5615)]	high
10/10/2023	[Oracle Linux 8 : libvpx (ELSA-2023-5537)]	high
10/10/2023	[Slackware Linux 15.0 / current libnotify Vulnerability (SSA:2023-283-02)]	high
10/10/2023	[Slackware Linux 15.0 / current libcue Vulnerability (SSA:2023-283-01)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Tue, 10 Oct 2023
Cacti 1.2.24 Command Injection
Cacti version 1.2.24 authenticated command injection exploit that uses SNMP options.
- Link
—
” “Tue, 10 Oct 2023
BoidCMS 2.0.0 Shell Upload
BoidCMS versions 2.0.0 and below suffer from a remote shell upload vulnerability.
- Link
—
” “Tue, 10 Oct 2023
Webedition CMS 2.9.8.8 Server-Side Request Forgery
Webedition CMS version 2.9.8.8 suffers from a blind server-side request forgery vulnerability.
- Link
—
” “Tue, 10 Oct 2023
OpenPLC WebServer 3 Denial Of Service
OpenPLC WebServer version 3 suffers from a denial of service vulnerability.
- Link
—
” “Tue, 10 Oct 2023
Atcom 2.7.x.x Command Injection
Atcom version 2.7.x.x suffers from an authenticated remote code injection vulnerability.
- Link
—
” “Tue, 10 Oct 2023
WordPress Sonaar Music 4.7 Cross Site Scripting
WordPress Sonaar Music plugin version 4.7 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Tue, 10 Oct 2023
Coppermine Gallery 1.6.25 Remote Code Execution
Coppermine Gallery version 1.6.25 remote code execution exploit.
- Link
—
” “Tue, 10 Oct 2023
Minio 2022-07-29T19-40-48Z Path Traversal
Minio version 2022-07-29T19-40-48Z suffers from a path traversal vulnerability.
- Link
—
” “Tue, 10 Oct 2023
WordPress Masterstudy LMS 3.0.17 Account Creation
WordPress Masterstudy LMS plugin version 3.0.17 suffers from an unauthenticated instructor account creation vulnerability.
- Link
—
” “Tue, 10 Oct 2023
Microsoft Windows 11 apds.dll DLL Hijacking
Microsoft Windows 11 apds.dll DLL hijacking exploit.
- Link
—
” “Tue, 10 Oct 2023
GLPI GZIP(Py3) 9.4.5 Remote Code Execution
GLPI GZIP(Py3) version 9.4.5 suffers from a remote code execution vulnerability.
- Link
—
” “Mon, 09 Oct 2023

Kibana Prototype Pollution / Remote Code Execution
Kibana versions prior to 7.6.3 suffer from a prototype pollution bug within the Upgrade Assistant. By setting a new constructor.prototype.sourceURL value you can execute arbitrary code. Code execution is possible through two different ways. Either by sending data directly to Elastic, or using Kibana to submit the same queries. Either method enters the polluted prototype for Kibana to read. Kibana will either need to be restarted, or collection happens (unknown time) for the payload to execute. Once it does, cleanup must delete the .kibana_1 index for Kibana to restart successfully. Once a callback does occur, cleanup will happen allowing Kibana to be successfully restarted on next attempt.
- Link
—
” “Mon, 09 Oct 2023
eClass Junior 4.0 SQL Injection
eClass Junior version 4.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 09 Oct 2023
eClass IP 2.5 SQL Injection
eClass IP version 2.5 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 09 Oct 2023
Chicv Management System Login 4.5.6 Insecure Direct Object Reference
Chicv Management System Login version 4.5.6 suffers from an insecure direct object reference vulnerability.
- Link
—
” “Mon, 09 Oct 2023
Aicte India LMS 3.0 Cross Site Scripting
Aicte India LMS version 3.0 suffers from a cross site scripting vulnerability.
- Link
—
” “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

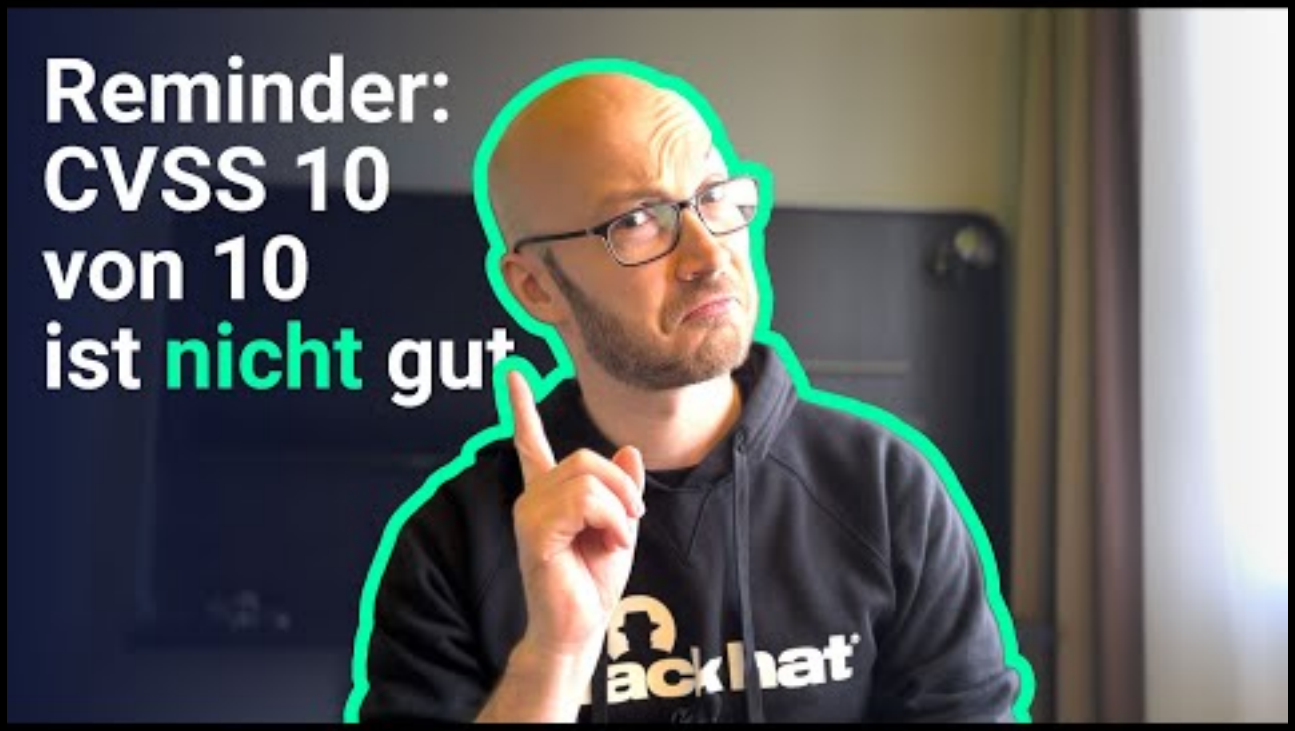
edgetpu_pin_user_pages Race Condition
There is a race condition in edgetpu_pin_user_pages which is reachable from some unprivileged contexts, including the Camera app, or the Google Meet app.
- Link
—
” “Wed, 04 Oct 2023
Progress Software WS_FTP Unauthenticated Remote Code Execution
This Metasploit module 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
—
”

0-Day

Die Hacks der Woche

mit Martin Haunschmid

In der IT-Security ist 10 von 10 NICHT IMMER etwas Gutes



Zum Youtube Video

Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-08	Volex PLC	[GBR]	Link
2023-10-07	Centre hospitalier de l'Ouest Vosgien	[FRA]	Link
2023-10-06	Clinique universitaire de Francfort	[DEU]	Link
2023-10-05	Dansk Scanning	[DNK]	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-Grupppe	Webseite
2023-10-11	[We monetize your corporate access]	everest	Link
2023-10-09	[Metro Transit]	play	Link
2023-10-01	[Effigest Capital Services]	noescape	Link
2023-10-10	[Alliance Virgil Roberts Leadership Academy]	snatch	Link
2023-10-10	[foremostgroups.com]	lockbit3	Link
2023-10-10	[National Health Mission. Department of Health & Family Welfare, Govt. of U.P]	knight	Link
2023-10-10	[mountstmarys]	cuba	Link
2023-10-10	[ExdionInsurance]	8base	Link
2023-10-10	[National Health Mission. Department of Heath & Family Welfare, Govt. of U.P]	knight	Link
2023-10-01	[Elbe-Obst Fruchtverarbeitung GmbH]	noescape	Link
2023-10-03	[Ordine Degli Psicologi Della Lombardia]	noescape	Link
2023-10-09	[Saltire Energy]	play	Link
2023-10-09	[Starr Finley]	play	Link
2023-10-09	[WCM Europe]	play	Link
2023-10-09	[NachtExpress Austria GmbH]	play	Link
2023-10-09	[Centek industries]	play	Link
2023-10-09	[M??? T??????]	play	Link
2023-10-10	[Hughes Gill Cochrane Tinetti]	play	Link
2023-10-01	[Penfield Fire Co]	noescape	Link
2023-10-01	[Centre Du Sablon]	noescape	Link
2023-10-06	[GEACAM]	noescape	Link
2023-10-09	[Guhring was hacked. Thousands of confidential files stolen.]	knight	Link
2023-10-09	[Wyndemere Senior Care, LLC]	alphv	Link
2023-10-09	[First Judicial Circuit - Florida Court]	alphv	Link
2023-10-09	[atlantatech.edu]	lockbit3	Link
2023-10-09	[starplast.ft]	lockbit3	Link
2023-10-09	[WT PARTNERSHIP]	qilin	Link
2023-10-09	[Superline - Press Release]	monti	Link
2023-10-09	[dothanhauto.com]	lockbit3	Link
2023-10-09	[vsmpo-tirus.com]	lockbit3	Link
2023-10-09	[Law Society of South Africa]	alphv	Link
2023-10-09	[enerjet.com.pe]	lockbit3	Link
2023-10-09	[i-Can Advisory Group inc]	alphv	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[picosoft.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.