Cybersecurity Morgenreport

Ausgabe: 20231219

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! Botnetz InfectedSlurs hat es auf Qnap NAS abgesehen
Eine Sicherheitslücke in der IP-Kamera-Software VioStor NVR auf Netzwerkspeichern von Qnap dient als Schlupfloch für Malware.
- Link

—

Sicherheitsupdates: Fortinet schützt Firewalls & Co. vor möglichen Attacken
Der Netzwerkausrüster Fortinet hat in mehreren Produkten gefährliche Lücken geschlossen.
- Link

—

Squid-Proxy: Denial of Service durch Endlosschleife
Schickt ein Angreifer einen präparierten HTTP-Header an den Proxy-Server, kann er ihn durch eine unkontrollierte Rekursion zum Stillstand bringen.
- Link

—

Zoom behebt Sicherheitslücken unter Windows, Android und iOS
Durch ungenügende Zugriffskontrolle, Verschlüsselungsprobleme und Pfadmanipulation konnten Angreifer sich zusätzliche Rechte verschaffen.
- Link

—

Patchday: Adobe schließt 185 Sicherheitslücken in Experience Manager
Angreifer können Systeme mit Anwendungen von Adobe ins Visier nehmen. Nun hat der Softwarehersteller Schwachstellen geschlossen.
- Link

—

Patchday Microsoft: Outlook kann sich an Schadcode-E-Mail verschlucken
Microsoft hat wichtige Sicherheitsupdates für Azure, Defender & Co. veröffentlicht. Bislang soll es keine Attacken geben.
- Link

—

Sicherheitsupdate Apache Struts: Uploadfunktion kann Schadcode passieren lassen
Eine kritische Schwachstelle bedroht das Open-Source-Framework Apache Struts.
- Link

—

WordPress Elementor: Halbgarer Sicherheitspatch gefährdete Millionen Websites
Es gibt wichtige Sicherheitsupdates für die WordPress-Plug-ins Backup Migration und Elementor.
- Link

—

Patchday: 15 Sicherheitswarnungen von SAP
Am Dezember-Patchday hat SAP 15 neue Sicherheitsmitteilungen herausgegeben. Sie thematisieren teils kritische Lücken.
- Link

—

Bluetooth-Lücke: Tastenanschläge in Android, Linux, iOS und macOS einschleusbar
Eine Sicherheitslücke in Bluetooth-Stacks erlaubt Angreifern, Tastenanschläge einzuschmuggeln. Unter Android, iOS, Linux und macOS.
- 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-2023-5360	0.968720000	0.996320000	Link
CVE-2023-4966	0.917920000	0.986830000	Link
CVE-2023-46747	0.965530000	0.995100000	Link
CVE-2023-46604	0.968050000	0.996050000	Link
CVE-2023-42793	0.972640000	0.998190000	Link
CVE-2023-38035	0.970940000	0.997240000	Link
CVE-2023-35078	0.953010000	0.991780000	Link
CVE-2023-34634	0.900470000	0.985230000	Link
CVE-2023-34039	0.928890000	0.988160000	Link
CVE-2023-33246	0.971220000	0.997420000	Link
CVE-2023-32315	0.961510000	0.993720000	Link
CVE-2023-30625	0.941420000	0.989750000	Link
CVE-2023-30013	0.925700000	0.987810000	Link
CVE-2023-28771	0.923800000	0.987590000	Link
CVE-2023-27524	0.906990000	0.985610000	Link
CVE-2023-27372	0.971560000	0.997580000	Link
CVE-2023-27350	0.972290000	0.997990000	Link
CVE-2023-26469	0.933320000	0.988700000	Link
CVE-2023-26360	0.934340000	0.988830000	Link
CVE-2023-25717	0.962820000	0.994090000	Link
CVE-2023-25194	0.908370000	0.985750000	Link
CVE-2023-2479	0.958820000	0.993110000	Link
CVE-2023-24489	0.967670000	0.995930000	Link
CVE-2023-22518	0.967630000	0.995920000	Link
CVE-2023-22515	0.955290000	0.992300000	Link
CVE-2023-21839	0.960570000	0.993480000	Link
CVE-2023-21823	0.955130000	0.992240000	Link
CVE-2023-21554	0.961220000	0.993620000	Link
CVE-2023-20887	0.957180000	0.992700000	Link
CVE-2023-1671	0.952600000	0.991690000	Link
CVE-2023-0669	0.966690000	0.995500000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 18 Dec 2023

[NEU] [hoch] Zabbix: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder Code auszuführen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] Atlassian Produkte: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Atlassian Bitbucket, Atlassian Confluence und Atlassian Jira Software ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] IBM InfoSphere Information Server: Mehrere Schwachstellen
Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in IBM InfoSphere Information Server ausnutzen, um einen Denial of Service Angriff durchzuführen, seine Privilegien zu erweitern oder vertrauliche Daten einzusehen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen
Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] Intel Prozessoren: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Intel Prozessoren ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern oder Informationen offenzulegen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [kritisch] Apache Struts: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Struts ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 18 Dec 2023
[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung
Ein Angreifer in Funk-Reichweite kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 15 Dec 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial of Service Angriff durchzuführen und Daten zu manipulieren.
- Link

—

Fri, 15 Dec 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Fri, 15 Dec 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder sonstige Auswirkungen zu verursachen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] Xen: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Xen ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Fri, 15 Dec 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 einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Fri, 15 Dec 2023
[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/18/2023	[Backup Migration Plugin for WordPress < 1.3.8 Remote Code Execution]	critical
12/18/2023	[GLSA-202312-01 : Leptonica: Multiple Vulnerabilities]	critical
12/18/2023	[VMware vRealize Network Insight (vRNI) Multiple Vulnerabilities (VMSA-2022-0031)]	critical
12/18/2023	[QNAP QTS / QuTS hero Vulnerabilities in Samba (QSA-23-20)]	critical
12/18/2023	[Microsoft SharePoint Authentication Bypass (CVE-2023-29357)]	critical
12/18/2023	[Amazon Linux 2023 : openssh, openssh-clients, openssh-keycat (ALAS2023-2023-462)]	critical
12/18/2023	[Amazon Linux 2 : openssh (ALAS-2023-2376)]	critical
12/18/2023	[Mitsubishi MELSEC-Q Series C Controller Module Denial of Service and Malicious Code Execution (CVE-2021-29998)]	critical
12/16/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:4883-1)]	critical
12/16/2023	[Fedora 38 : perl / perl-Devel-Cover / perl-PAR-Packer / polymake (2023-9ef8a60a05)]	critical
12/15/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:4882-1)]	critical
12/18/2023	[Joomla! 5.x < 5.0.1 Information Disclosure]	high
12/18/2023	[Joomla! 1.6.x < 4.4.1 Information Disclosure]	high
12/18/2023	[Debian DLA-3691-1 : spip - LTS security update]	high
12/18/2023	[Debian DSA-5579-1 : freeimage - security update]	high
12/18/2023	[AlmaLinux 9 : fence-agents (ALSA-2023:7753)]	high
12/18/2023	[Siemens (CVE-2023-46156)]	high
12/17/2023	[Debian DLA-3690-1 : intel-microcode - LTS security update]	high
12/17/2023	[Fedora 39 : unrealircd (2023-cfe04c6093)]	high
12/17/2023	[Fedora 38 : unrealircd (2023-239f057b33)]	high
12/16/2023	[Fedora 38 : seamonkey (2023-deb5cf6515)]	high
12/15/2023	[Oracle Linux 9 : postgresql (ELSA-2023-7784)]	high
12/15/2023	[Debian DSA-5578-1 : ghostscript - security update]	high
12/15/2023	[Fedora 38 : chromium (2023-3d9f7ca27f)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Fri, 15 Dec 2023
RTPEngine mr11.5.1.6 Denial Of Service
RTPEngine version mr11.5.1.6 suffers from a denial of service vulnerability via DTLS Hello packets during call initiation.
- Link
—
” “Fri, 15 Dec 2023
PKP-WAL 3.4.0-3 Remote Code Execution
PKP Web Application Library (PKP-WAL) versions 3.4.0-3 and below, as used in Open Journal Systems (OJS), Open Monograph Press (OMP), and Open Preprint Systems (OPS) before versions 3.4.0-4 or 3.3.0-16, suffer from a NativeImportExportPlugin related remote code execution vulnerability.
- Link
—
” “Fri, 15 Dec 2023
Asterisk 20.1.0 Denial Of Service
When handling DTLS-SRTP for media setup, Asterisk version 20.1.0 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.
- Link
—
” “Fri, 15 Dec 2023
osCommerce 4.13-60075 Shell Upload
osCommerce version 4.13-60075 suffers from a remote shell upload vulnerability.
- Link
—
” “Thu, 14 Dec 2023
Chrome V8 Sandbox Escape
Proof of concept exploit for a new technique to escape from the Chrome V8 sandbox.
- Link
—
” “Thu, 14 Dec 2023
Chrome V8 Type Confusion / New Sandbox Escape
Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap corruption via a crafted HTML page. This variant of the exploit applies a new technique to escape the sandbox.
- Link
—
” “Thu, 14 Dec 2023
Chrome V8 JIT XOR Arbitrary Code Execution
Chrome V8 proof of concept exploit for CVE-2021-21220. The specific flaw exists within the implementation of XOR operation when executed within JIT compiled code.
- Link
—
” “Thu, 14 Dec 2023
Chrome V8 Type Confusion
Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- Link
—
” “Thu, 14 Dec 2023
Windows Kernel Race Conditions
The Microsoft Windows Kernel has an issue with bad locking in registry virtualization that can result in race conditions.
- Link
—
” “Wed, 13 Dec 2023

PDF24 Creator 11.15.1 Local Privilege Escalation
PDF24 Creator versions 11.15.1 and below suffer from a local privilege escalation vulnerability via the MSI installer.
- Link
—
” “Wed, 13 Dec 2023
One Identity Password Manager Kiosk Escape Privilege Escalation
One Identity Password Manager versions prior to 5.13.1 suffer from a kiosk escape privilege escalation vulnerability.
- Link
—
” “Wed, 13 Dec 2023
Atos Unify OpenScape Authentication Bypass / Remote Code Execution
Atos Unify OpenScape Session Border Controller (SBC) versions before V10 R3.4.0, Branch versions before V10 R3.4.0, and BCF versions before V10 R10.12.00 and V10 R11.05.02 suffer from an argument injection vulnerability that can lead to unauthenticated remote code execution and authentication bypass.
- Link
—
” “Wed, 13 Dec 2023
Anveo Mobile User Enumeration / Missing Certificate Validation
Anveo Mobile application version 10.0.0.359 and server version 11.0.0.5 suffer from missing certificate validation and user enumeration vulnerabilities.
- Link
—
” “Tue, 12 Dec 2023
Splunk XSLT Upload Remote Code Execution
This Metasploit module exploits a remote code execution vulnerability in Splunk Enterprise. The affected versions include 9.0.x before 9.0.7 and 9.1.x before 9.1.2. The exploitation process leverages a weakness in the XSLT transformation functionality of Splunk. Successful exploitation requires valid credentials, typically admin:changeme by default. The exploit involves uploading a malicious XSLT file to the target system. This file, when processed by the vulnerable Splunk server, leads to the execution of arbitrary code. The module then utilizes the runshellscript capability in Splunk to execute the payload, which can be tailored to establish a reverse shell. This provides the attacker with remote control over the compromised Splunk instance. The module is designed to work seamlessly, ensuring successful exploitation under the right conditions.
- Link
—
” “Tue, 12 Dec 2023
WordPress Backup Migration 1.3.7 Remote Code Execution
WordPress Backup Migration plugin versions 1.3.7 and below suffer from a remote code execution vulnerability.
- Link
—
” “Mon, 11 Dec 2023
WordPress Contact Form To Any API 1.1.6 Cross Site Request Forgery
WordPress Contact Form to Any API plugin versions 1.1.6 and below suffer from a cross site request forgery vulnerability.
- Link
—
” “Mon, 11 Dec 2023
WordPress Bravo Translate 1.2 SQL Injection
WordPress Bravo Translate plugin versions 1.2 and below suffer from a remote SQL injection vulnerability.
- Link
—
” “Mon, 11 Dec 2023
WordPress TextMe SMS 1.9.0 Cross Site Request Forgery
WordPress TextMe SMS plugin versions 1.9.0 and below suffer from a cross site request forgery vulnerability.
- Link
—
” “Sat, 09 Dec 2023
libcue 2.2.1 Out-Of-Bounds Access
libcue provides an API for parsing and extracting data from CUE sheets. Versions 2.2.1 and prior are vulnerable to out-of-bounds array access. A user of the GNOME desktop environment can be exploited by downloading a

cue sheet from a malicious webpage. Because the file is saved to ~/Downloads, it is then automatically scanned by tracker-miners. And because it has a .cue filename extension, tracker-miners use libcue to parse the file. The file exploits the vulnerability in libcue to gain code execution. This issue is patched in version 2.3.0. This particular archive holds three proof of concept exploits.
- Link
—
” “Fri, 08 Dec 2023
Microsoft Defender Anti-Malware PowerShell API Arbitrary Code Execution
Microsoft Defender API and PowerShell APIs suffer from an arbitrary code execution due to a flaw in powershell not handling user provided input that contains a semicolon.
- Link
—
” “Fri, 08 Dec 2023
ISPConfig 3.2.11 PHP Code Injection
ISPConfig versions 4.2.11 and below suffer from a PHP code injection vulnerability in language_edit.php.
- Link
—
” “Fri, 08 Dec 2023
osCommerce 4 SQL Injection
osCommerce version 4 suffers from a remote SQL injection vulnerability.
- Link
—
” “Fri, 08 Dec 2023
Kopage Website Builder 4.4.15 Shell Upload
Kopage Website Builder version 4.4.15 appears to suffer from a remote shell upload vulnerability.
- Link
—
” “Fri, 08 Dec 2023
Windows Kernel Information Disclosure
The Microsoft Windows Kernel has a time-of-check / time-of-use issue in verifying layered key security which may lead to information disclosure from privileged registry keys.
- Link
—
” “Fri, 08 Dec 2023
Arm Mali CSF Overflow / Use-After-Free
Arm Mali CSF has a refcount overflow bugfix in r43p0 that was misclassified as a memory leak fix.
- Link
—
”

0-Days der letzten 5 Tage

“Fri, 15 Dec 2023
ZDI-23-1799: Ivanti Avalanche Incorrect Default Permissions Local Privilege Escalation Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1798: PaperCut NG Uncontrolled Search Path Element Local Privilege Escalation Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1797: Schneider Electric C-Bus Toolkit TransferCommand Exposed Dangerous Method Remote Code Execution Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1796: Schneider Electric C-Bus Toolkit FileCommand Directory Traversal Remote Code Execution Vulnerability
- Link

—
” “Fri, 15 Dec 2023
ZDI-23-1795: Schneider Electric EcoStruxure Power Monitoring Expert GetFilteredSinkProvider Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1794: Schneider Electric APC Easy UPS Online deletePdfReportFile Directory Traversal Denial-of-Service Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1793: Delta Electronics DOPSoft DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Fri, 15 Dec 2023
ZDI-23-1792: Microsoft Windows win32kfull UMPDDrvCopyBits Use-After-Free Local Privilege Escalation Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

Ihr habt WAS in eure Züge programmiert!?

Zum Youtube Video

Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2023-12-14	Verocard	[BRA]	Link
2023-12-13	Limburg.net	[BEL]	Link
2023-12-13	London Public Library	[CAN]	Link
2023-12-13	Agência Nacional de Águas e Saneamento Básico (ANA)	[BRA]	Link
2023-12-13	VF Corp	[USA]	Link
2023-12-13	MongoDB	[USA]	Link
2023-12-12	District de March	[CHE]	Link
2023-12-12	Hotelplan UK	[GBR]	Link
2023-12-11	Banque centrale du Lesotho	[LSO]	Link
2023-12-11	Milton Town School District (MTSD)	[USA]	Link
2023-12-10	Jysk Energi	[DNK]	Link
2023-12-10	EasyPark	[NLD]	Link
2023-12-10	CACG (Compagnie d'Aménagement des Coteaux de Gascogne)	[FRA]	Link
2023-12-09	Mairie d'Ozoir-la-Ferrière	[FRA]	Link
2023-12-08	Province des îles Loyauté	[NCL]	Link
2023-12-08	WestPole	[ITA]	Link
2023-12-08	Coaxis	[FRA]	Link
2023-12-07	Aqualectra	[CUW]	Link
2023-12-07	Université de Wollongong	[AUS]	Link
2023-12-07	Prefeitura de Poços de Caldas	[BRA]	Link
2023-12-07	Hinsdale School District	[USA]	Link
2023-12-06	Nissan Oceania	[AUS]	Link
2023-12-06	Gouvernement du Yucatan	[MEX]	Link
2023-12-06	Université de Sherbrooke	[CAN]	Link
2023-12-06	Glendale Unified School District	[USA]	Link
2023-12-06	Groveport Madison School District	[USA]	Link
2023-12-05	Dameron Hospital	[USA]	Link
2023-12-05	Gräbener Maschinentechnik	[DEU]	Link
2023-12-04	Caribbean Community (Caricom) Secretariat	[GUY]	Link
2023-12-01	Communauté de communes du Pays du Neubourg	[FRA]	Link

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-19	[Kauno Technologijos Universitetas]	rhysida	Link
2023-12-18	[Blackstone Valley Community Health Care]	hunters	Link
2023-12-18	[Richard Harris Personal Injury Law Firm]	play	Link
2023-12-18	[Schoepe Display]	play	Link
2023-12-18	[Waldner's]	play	Link
2023-12-18	[Succes Schoonmaak]	play	Link
2023-12-18	[DYWIDAG-Systems & American Transportation]	play	Link
2023-12-18	[C?????z????]	play	Link
2023-12-18	[The CM Paula]	play	Link
2023-12-18	[parat-technology.com]	lockbit3	Link
2023-12-18	[Viking Therapeutics reported to the SEC following a breach]	alphv	Link
2023-12-18	[naandanjain.com]	toufan	Link
2023-12-18	[LAJOLLAGROUP]	cactus	Link
2023-12-18	[Ta-Supply.com]	toufan	Link
2023-12-18	[Electrical Connections]	bianlian	Link
2023-12-18	[navitaspet.com]	blackbasta	Link
2023-12-18	[vyera.com]	blackbasta	Link
2023-12-18	[hallidays.co.uk]	blackbasta	Link
2023-12-17	[techno-rezef.com]	toufan	Link
2023-12-17	[curver.com]	toufan	Link
2023-12-17	[dorot.com]	toufan	Link
2023-12-17	[graf.co.il]	toufan	Link
2023-12-17	[brother.co.il]	toufan	Link
2023-12-17	[ATCO Products Inc]	medusa	Link
2023-12-17	[Biomatrix LLC]	medusa	Link
2023-12-17	[TechKids aka MindX]	raznatovic	Link
2023-12-17	[SKF.com]	raznatovic	Link
2023-12-17	[Colonial Pipeline]	raznatovic	Link
2023-12-17	[rodo.co.uk]	lockbit3	Link
2023-12-16	[E & J Gallo Winery]	alphv	Link
2023-12-14	[Kraft Foods]	snatch	Link
2023-12-14	[Spaulding Clinical]	snatch	Link
2023-12-16	[Crace Medical Centre]	knight	Link
2023-12-16	[DSG-US.COM]	clop	Link
2023-12-16	[New York School of Interior Design]	incransom	Link
2023-12-16	[CTS]	cactus	Link
2023-12-16	[kohlwholesale.com]	blackbasta	Link
2023-12-16	[Insidesource]	8base	Link
2023-12-15	[hebeler.com]	lockbit3	Link
2023-12-15	[Nexiga]	akira	Link
2023-12-07	[CIE]	cactus	Link
2023-12-07	[NNDOMAIN]	cactus	Link
2023-12-11	[ISC]	cactus	Link
2023-12-13	[DILLARD]	cactus	Link
2023-12-15	[Fred Hutchinson Cancer Research Center]	hunters	Link
2023-12-14	[bemes.com]	lockbit3	Link
2023-12-14	[mcs360.com]	lockbit3	Link
2023-12-14	[goldwind.com]	lockbit3	Link
2023-12-14	[converzemedia.com]	lockbit3	Link
2023-12-14	[rpassoc.com]	lockbit3	Link
2023-12-14	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry]	bianlian	Link
2023-12-14	[Commonwealth Capital]	bianlian	Link
2023-12-14	[Greenbox Loans Inc.]	bianlian	Link
2023-12-14	[Hyman Hayes Associates]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-14	[grandrapidswomenshealth.com]	lockbit3	Link
2023-12-14	[pcli.com]	lockbit3	Link
2023-12-13	[austen-it.com]	lockbit3	Link
2023-12-08	[Akir Metal San Tic Ltd ti was hacked. All confidential information was stolen]	knight	Link
2023-12-13	[Gaido-fintzen.com]	cloak	Link
2023-12-13	[DAIHO INDUSTRIAL Co.,Ltd.]	knight	Link
2023-12-13	[cityofdefiance.com]	knight	Link
2023-12-13	[Heart of Texas Region MHMR]	dragonforce	Link
2023-12-13	[PCTEL]	dragonforce	Link
2023-12-13	[Agl Welding Supply]	dragonforce	Link
2023-12-13	[Grayhill]	dragonforce	Link
2023-12-13	[Leedarson Lighting]	dragonforce	Link
2023-12-13	[Coca-Cola Singapore]	dragonforce	Link
2023-12-13	[Shorts]	dragonforce	Link
2023-12-13	[World Emblem International]	dragonforce	Link
2023-12-13	[The GBUAHN]	dragonforce	Link
2023-12-13	[Baden]	dragonforce	Link
2023-12-13	[Dafiti Argentina]	dragonforce	Link
2023-12-13	[Lunacon Construction Group]	dragonforce	Link
2023-12-13	[Tglt]	dragonforce	Link
2023-12-13	[Seven Seas]	dragonforce	Link
2023-12-13	[Decina]	dragonforce	Link
2023-12-13	[Cooper Research Technology]	dragonforce	Link
2023-12-13	[Greater Cincinnati Behavioral Health]	dragonforce	Link
2023-12-13	[ccadm.org]	lockbit3	Link
2023-12-13	[dawsongroup.co.uk]	lockbit3	Link
2023-12-13	[altezze.com.mx]	lockbit3	Link
2023-12-13	[Tulane University]	meow	Link
2023-12-13	[thirdstreetbrewhouse.com carolinabeveragegroup.com]	blackbasta	Link
2023-12-13	[Advantage Group International]	alphv	Link
2023-12-13	[Dameron Hospital]	ransomhouse	Link
2023-12-13	[agy.com]	blackbasta	Link
2023-12-13	[alexander-dennis.com]	blackbasta	Link
2023-12-13	[Dillard Door & Security]	cactus	Link
2023-12-13	[cms.law]	lockbit3	Link
2023-12-13	[SBK Real Estate]	8base	Link
2023-12-13	[CACG]	8base	Link
2023-12-13	[VAC-U-MAX]	8base	Link
2023-12-13	[Hawkins Sales]	8base	Link
2023-12-13	[William Jackson Food Group]	8base	Link
2023-12-13	[Groupe PROMOBE]	8base	Link
2023-12-13	[Soethoudt metaalbewerking b.v.]	8base	Link
2023-12-13	[REUS MOBILITAT I SERVEIS]	8base	Link
2023-12-13	[Tim Davies Landscaping]	8base	Link
2023-12-12	[King Aerospace, Inc.]	incransom	Link
2023-12-12	[GlobalSpec]	play	Link
2023-12-12	[dena.de]	lockbit3	Link
2023-12-12	[woodruffenterprises.com]	threeam	Link
2023-12-12	[shareharris.com]	threeam	Link
2023-12-12	[SmartWave Technologies]	akira	Link
2023-12-12	[Mitrani Caballero Ojam & Ruiz Moreno - Abogados]	akira	Link
2023-12-12	[The Teaching Company, LLC]	akira	Link
2023-12-12	[Memorial Sloan Kettering Cancer Center]	meow	Link
2023-12-12	[petrotec.com.qa]	lockbit3	Link
2023-12-12	[tradewindscorp-insbrok.com]	lockbit3	Link
2023-12-12	[airtechthelong.com.vn]	lockbit3	Link
2023-12-12	[kitahirosima.jp]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-12	[Grupo Jose Alves]	rhysida	Link
2023-12-12	[Insomniac Games]	rhysida	Link
2023-12-11	[phillipsglobal.us]	lockbit3	Link
2023-12-11	[greenbriersportingclub.com]	lockbit3	Link
2023-12-11	[ipp-sa.com]	lockbit3	Link
2023-12-11	[r-ab.de]	lockbit3	Link
2023-12-11	[Azienda USL di Modena]	hunters	Link
2023-12-11	[igt.nl]	lockbit3	Link
2023-12-01	[Bayer Heritage Federal Credit Union]	lorenz	Link
2023-12-11	[MSD Information technology]	akira	Link
2023-12-11	[Goiasa]	akira	Link
2023-12-11	[Hinsdale School District]	medusa	Link
2023-12-11	[Independent Recovery Resources, Inc.]	bianlian	Link
2023-12-11	[Studio MF]	akira	Link
2023-12-11	[zailaboratory.com]	lockbit3	Link
2023-12-11	[ISC Consulting Engineers]	cactus	Link
2023-12-11	[The Glendale Unified School District]	medusa	Link
2023-12-10	[pronatindustries.com]	lockbit3	Link
2023-12-10	[policia.gob.pe]	lockbit3	Link
2023-12-10	[Holding Slovenske elektarne]	rhysida	Link
2023-12-10	[Hse]	rhysida	Link
2023-12-09	[Qatar Racing and Equestrian Club]	rhysida	Link
2023-12-09	[Graphic Solutions Group Inc (US)]	daixin	Link
2023-12-09	[OpTransRights - 2]	siegedsec	Link
2023-12-09	[Telerad]	siegedsec	Link
2023-12-09	[Technical University of Mombasa]	siegedsec	Link
2023-12-09	[National Office for centralized procurement]	siegedsec	Link
2023-12-09	[Portland Government & United states government]	siegedsec	Link
2023-12-09	[Staples]	siegedsec	Link
2023-12-09	[Deqing County]	siegedsec	Link
2023-12-09	[Colombian National Registry]	siegedsec	Link
2023-12-09	[HMW - Press Release]	monti	Link
2023-12-08	[livanova.com]	lockbit3	Link
2023-12-04	[Jerry Pate Energy (hack from Saltmarsh Financial Advisors)]	snatch	Link
2023-12-08	[GOLFZON]	blacksuit	Link
2023-12-08	[aw-lawyers.com]	lockbit3	Link
2023-12-08	[midlandindustries.com]	lockbit3	Link
2023-12-08	[Travian Games]	rhysida	Link
2023-12-08	[Tcman]	rhysida	Link
2023-12-07	[California Innovations]	play	Link
2023-12-07	[SMRT]	play	Link
2023-12-07	[Intrepid Sea, Air & Space Museum]	play	Link
2023-12-07	[Postworks]	play	Link
2023-12-07	[PLS Logistics]	play	Link
2023-12-07	[Ridge Vineyards]	play	Link
2023-12-07	[AJO]	play	Link
2023-12-07	[PHIBRO GMBH]	play	Link
2023-12-07	[denave.com]	lockbit3	Link
2023-12-07	[Precision Technologies Group Ltd]	incransom	Link
2023-12-07	[Silvent North America]	play	Link
2023-12-07	[GreenWaste Recovery]	play	Link
2023-12-07	[Burton Wire & Cable]	play	Link
2023-12-07	[Capespan]	play	Link
2023-12-07	[Becker Furniture World]	play	Link
2023-12-07	[Payne Hicks Beach]	play	Link
2023-12-07	[Vitro Plus]	play	Link
2023-12-07	[GVM]	play	Link
2023-12-07	[Planbox]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-07	[AG Consulting Engineering]	play	Link
2023-12-07	[Greater Richmond Transit]	play	Link
2023-12-07	[Kuriyama of America]	play	Link
2023-12-07	[bluewaterstt.com]	lockbit3	Link
2023-12-07	[omegapainclinic.com]	lockbit3	Link
2023-12-07	[AMCO Proteins]	bianlian	Link
2023-12-07	[SML Group]	bianlian	Link
2023-12-07	[stormtech]	metaencryptor	Link
2023-12-07	[Garda]	metaencryptor	Link
2023-12-07	[Tri-city Medical Center]	incransom	Link
2023-12-07	[Tasteful Selections]	akira	Link
2023-12-07	[Ware Manufacturing]	qilin	Link
2023-12-07	[Neurology Center of Nevada]	qilin	Link
2023-12-07	[CIE Automotive]	cactus	Link
2023-12-07	[National Nail Corp]	cactus	Link
2023-12-07	[citizenswv.com]	lockbit3	Link
2023-12-07	[directradiology.com]	lockbit3	Link
2023-12-07	[signiflow.com]	lockbit3	Link
2023-12-07	[bpce.com]	lockbit3	Link
2023-12-07	[hopto.com]	lockbit3	Link
2023-12-07	[usherbrooke.ca]	lockbit3	Link
2023-12-07	[Visan]	8base	Link
2023-12-07	[Tryax Realty Management - Press Release]	monti	Link
2023-12-06	[Campbell County Schools]	medusa	Link
2023-12-06	[Deutsche Energie-Agentur]	alphv	Link
2023-12-06	[Compass Group Italia]	akira	Link
2023-12-06	[Aqualectra Holdings]	akira	Link
2023-12-06	[Acero Engineering]	bianlian	Link
2023-12-06	[syrtech.com]	threeam	Link
2023-12-06	[ACCU Reference Medical Lab]	medusa	Link
2023-12-06	[Sagent]	medusa	Link
2023-12-06	[fpz.com]	lockbit3	Link
2023-12-06	[labelians.fr]	lockbit3	Link
2023-12-06	[polyclinique-cotentin.com]	lockbit3	Link
2023-12-06	[Lischkoff and Pitts, P.C.]	8base	Link
2023-12-06	[SMG Confrere]	8base	Link
2023-12-06	[Calgary TELUS Convention Centre]	8base	Link
2023-12-06	[astley.]	8base	Link
2023-12-05	[Henry Schein Inc - Henry's " LOST SHINE "]	alphv	Link
2023-12-05	[TraCS Florida FSU]	alphv	Link
2023-12-05	[aldoshoes.com]	lockbit3	Link
2023-12-05	[laprensani.com]	lockbit3	Link
2023-12-05	[mapc.org]	lockbit3	Link
2023-12-05	[ussignandmill.com]	threeam	Link
2023-12-05	[Rudolf-Venture Chemical Inc - Part 1]	monti	Link
2023-12-05	[Akumin]	bianlian	Link
2023-12-05	[CLATSKANIEPUD]	alphv	Link
2023-12-05	[restargp.com]	lockbit3	Link
2023-12-05	[concertus.co.uk]	abyss	Link
2023-12-05	[Bowden Barlow Law PA]	medusa	Link
2023-12-05	[Rosens Diversified Inc]	medusa	Link
2023-12-05	[Henry County Schools]	blacksuit	Link
2023-12-05	[fps.com]	blacksuit	Link
2023-12-04	[Full access to the school network USA]	everest	Link
2023-12-04	[CMS Communications]	qilin	Link
2023-12-04	[Tipalti]	alphv	Link
2023-12-04	[Great Lakes Technologies]	qilin	Link
2023-12-04	[Midea Carrier]	akira	Link
2023-12-04	[ychlccsc.edu.hk]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-04	[nlt.com]	blackbasta	Link
2023-12-04	[Getrix]	akira	Link
2023-12-04	[Evnhcmc]	alphv	Link
2023-12-03	[mirle.com.tw]	lockbit3	Link
2023-12-03	[Bern Hotels & Resorts]	akira	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox and Twitch, two of their affected cl]	alphv	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox, one of their affected clients, indi]	alphv	Link
2023-12-02	[Lisa Mayer CA, Professional Corporation]	alphv	Link
2023-12-02	[bboed.org]	lockbit3	Link
2023-12-01	[hnncsb.org]	lockbit3	Link
2023-12-01	[elsewedyelectric.com]	lockbit3	Link
2023-12-01	[Austal USA]	hunters	Link
2023-12-02	[inseinc.com]	blackbasta	Link
2023-12-02	[royaleinternational.com]	alphv	Link
2023-12-01	[Dörr Group]	alphv	Link
2023-12-01	[IRC Engineering]	alphv	Link
2023-12-01	[Hello Cristina from Law Offices of John E Hill]	monti	Link
2023-12-01	[Hello Jacobs from RVC]	monti	Link
2023-12-01	[Austal]	hunters	Link
2023-12-01	[St. Johns River Water Management District]	hunters	Link
2023-12-01	[Kellett & Bartholow PLLC]	incransom	Link
2023-12-01	[Centroedile Milano]	blacksuit	Link
2023-12-01	[Iptor]	akira	Link
2023-12-01	[farwickgrote.de]	cloak	Link
2023-12-01	[skncustoms.com]	cloak	Link
2023-12-01	[euro2000-spa.it]	cloak	Link
2023-12-01	[Thenewtrongroup.com]	cloak	Link
2023-12-01	[Bankofceylon.co.uk]	cloak	Link
2023-12-01	[carranza.on.ca]	cloak	Link
2023-12-01	[Agamatrix]	meow	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.