Cybersecurity Morgenreport

Ausgabe: 20230822

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 Zero-Day-Lücke in Ivanti Sentry geschlossen
Ivanti schließt in Sentry, vormals MobileIron Sentry, eine kritische Sicherheitslücke. Sie wird bereits angegriffen.
- Link

—

Angreifer können Sicherheitslücken in Junos OS zu kritischer Gefahr eskalieren
Das Netzwerkbetriebssystem Junos OS ist über mehrere Schwachstellen attackierbar. Dagegen abgesicherte Versionen stehen zum Download bereit.
- Link

—

Update bereits ausgespielt: Kritische Lücke in WinRAR erlaubte Code-Ausführung
Das verbreitete Kompressionstool WinRAR besaß in älteren Versionen eine schwere Lücke, die beliebige Codeausführung erlaubte. Die aktuelle Version schließt sie.
- Link

—

Sicherheitslösung: IBM Security Guardium als Einfallstor für Angreifer
Eine kritische Lücke bedroht Systeme mit IBM Security Guardium. Sicherheitspatches sind verfügbar.
- Link

—

Sicherheitsupdates: Root-Lücken bedrohen Cisco-Produkte
Es sind wichtige Sicherheitsupdates für unter anderem Cisco Unified Communications Manager und Prime Infrastructure erschienen.
- Link

—

Jetzt patchen! Citrix ShareFile im Visier von Angreifern
Unbekannte Angreifer nutzen eine kritische Sicherheitslücke in Citrix ShareFile StorageZones Controller aus. Updates sind verfügbar.
- Link

—

Lücken in Kennzeichenerkennungssoftware gefährden Axis-Überwachungskamera
Mehrere Sicherheitslücken in Software für Überwachungskameras von Axis gefährden Geräte.
- Link

—

Sicherheitslücken: Angreifer können Hintertüren in Datenzentren platzieren
Schwachstellen in Software von CyberPower und Dataprobe zur Energieüberwachung und -Verteilung gefährden Datenzentren.
- Link

—

Vielfältige Attacken auf Ivanti Enterprise Mobility Management möglich
Angreifer können Schadcode auf Systeme mit Ivanti EMM schieben und ausführen. Eine dagegen abgesicherte Version schafft Abhilfe.
- Link

—

Schadcode-Attacken via WLAN auf einige Automodelle von Ford möglich
Eine Schwachstelle im Infotainmentsystem gefährdet bestimmte Modellserien von Ford und Lincoln. Die Fahrsicherheit soll davon aber nicht beeinträchtigt sein.
- 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-2023-39143	0.921370000	0.985560000	Link
CVE-2023-3519	0.911990000	0.984710000	Link
CVE-2023-35078	0.965240000	0.994110000	Link
CVE-2023-34362	0.936790000	0.987590000	Link
CVE-2023-33246	0.963860000	0.993530000	Link
CVE-2023-28771	0.918810000	0.985320000	Link
CVE-2023-28121	0.937820000	0.987690000	Link
CVE-2023-27372	0.970840000	0.996600000	Link
CVE-2023-27350	0.971160000	0.996780000	Link
CVE-2023-25717	0.967140000	0.994930000	Link
CVE-2023-25194	0.924830000	0.985920000	Link
CVE-2023-24489	0.967300000	0.995000000	Link
CVE-2023-21839	0.961530000	0.992810000	Link
CVE-2023-21554	0.902620000	0.983880000	Link
CVE-2023-20887	0.960660000	0.992580000	Link
CVE-2023-0669	0.967490000	0.995100000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 21 Aug 2023
[NEU] [hoch] Moodle: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Sicherheitsmechanismen zu umgehen, Informationen offenzulegen und SQL-Injection- oder Cross-Site-Scripting-Angriffe durchzuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Denial-of-Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Speicher zu verändern und möglicherweise beliebigen Code auszuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code

auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und einen nicht spezifizierten Angriff durchzuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen und einen Denial of Service zu verursachen oder Daten zu manipulieren oder offenzulegen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und einen Denial-of-Service-Zustand zu verursachen
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, Speicher zu manipulieren und Sicherheitsmaßnahmen zu umgehen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen oder Sicherheitsmaßnahmen zu umgehen.
- Link

—

Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 21 Aug 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

—

Mon, 21 Aug 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
—
Mon, 21 Aug 2023
[UPDATE] [hoch] Mozilla Firefox und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Mon, 21 Aug 2023
[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.
- Link
—
Mon, 21 Aug 2023
[NEU] [hoch] genua genucenter: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in genua genucenter ausnutzen, um Informationen offenzulegen, Dateien zu manipulieren, um Cross-Site Scripting Angriffe durchzuführen oder um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Fri, 18 Aug 2023
[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Offenlegung von Informationen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um Informationen offenzulegen.
- Link
—
Fri, 18 Aug 2023
[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.
- Link
—
Fri, 18 Aug 2023
[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um Sicherheitsvorkehrungen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand herzustellen.
- Link
—
Fri, 18 Aug 2023
[UPDATE] [hoch] expat: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen
Ein Angreifer kann mehrere Schwachstellen in expat ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/21/2023	[openSUSE 15 Security Update : python-mitmproxy (openSUSE-SU-2023:0233-1)]	critical

Datum	Schwachstelle	Bewertung
8/21/2023	[openSUSE 15 Security Update : python-mitmproxy (openSUSE-SU-2023:0232-1)]	critical
8/20/2023	[Fedora 38 : chromium (2023-f8e94641dc)]	critical
8/19/2023	[Fedora 37 : nodejs16 / nodejs18 / nodejs20 (2023-18476abd7e)]	critical
8/19/2023	[openSUSE 15 Security Update : opensuse-welcome (openSUSE-SU-2023:0230-1)]	critical
8/19/2023	[Fedora 37 : chromium (2023-6c8de2cd15)]	critical
8/19/2023	[Fedora 37 : gerbv (2023-5f5bea627b)]	critical
8/19/2023	[SUSE SLES12 Security Update : nodejs18 (SUSE-SU-2023:3356-1)]	critical
8/19/2023	[SUSE SLES12 Security Update : nodejs16 (SUSE-SU-2023:3355-1)]	critical
8/18/2023	[Fedora 38 : trafficserver (2023-dcbfbf1396)]	critical
8/18/2023	[Debian DSA-5479-1 : chromium - security update]	critical
8/18/2023	[Ivanti Avalanche < 6.4.1 Multiple Vulnerabilities]	critical
8/21/2023	[Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6302-1)]	high
8/21/2023	[Jenkins plugins Multiple Vulnerabilities (2023-08-16)]	high
8/21/2023	[Security Updates for Microsoft SQL Server ODBC Driver (August 2023)]	high
8/20/2023	[Fedora 37 : libreswan (2023-dbc6d8a124)]	high
8/20/2023	[Fedora 38 : libreswan (2023-ddd6e6b49b)]	high
8/20/2023	[Fedora 38 : dotnet6.0 / dotnet7.0 (2023-cbc688b8ca)]	high
8/20/2023	[Fedora 37 : dotnet6.0 / dotnet7.0 (2023-25112489ab)]	high
8/19/2023	[Fedora 37 : java-1.8.0-openjdk (2023-a2922bf669)]	high
8/19/2023	[Fedora 38 : java-1.8.0-openjdk (2023-b3384af468)]	high
8/19/2023	[SUSE SLES15 Security Update : kernel-firmware (SUSE-SU-2023:3361-1)]	high
8/19/2023	[SUSE SLES12 Security Update : kernel-firmware (SUSE-SU-2023:3362-1)]	high
8/19/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel-firmware (SUSE-SU-2023:3360-1)]	high
8/18/2023	[Fedora 37 : webkitgtk (2023-19754c5a93)]	high
8/18/2023	[Fedora 38 : qt5-qtbase (2023-04d519d0b3)]	high
8/18/2023	[SUSE SLES12 Security Update : postgresql15 (SUSE-SU-2023:3345-1)]	high
8/18/2023	[SUSE SLES12 Security Update : postgresql12 (SUSE-SU-2023:3341-1)]	high
8/18/2023	[SUSE SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2023:3344-1)]	high
8/18/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2023:3348-1)]	high
8/18/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2023:3347-1)]	high
8/18/2023	[SUSE SLES12 Security Update : postgresql15 (SUSE-SU-2023:3342-1)]	high
8/18/2023	[SUSE SLES15 Security Update : postgresql12 (SUSE-SU-2023:3346-1)]	high
8/18/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:3349-1)]	high
8/18/2023	[SUSE SLES12 Security Update : postgresql15 (SUSE-SU-2023:3343-1)]	high
8/18/2023	[Debian DLA-3535-1 : unrar-nonfree - LTS security update]	high
8/18/2023	[Debian DLA-3534-1 : rar - LTS security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Mon, 21 Aug 2023
Jorani Remote Code Execution
This Metasploit module exploits an unauthenticated remote code execution vulnerability in Jorani versions prior to 1.0.2. It abuses log poisoning and redirection bypass via header spoofing and then it uses path traversal to trigger the vulnerability. It has been tested on Jorani 1.0.0.
- Link
—
” “Mon, 21 Aug 2023
Academy LMS 6.1 Cross Site Scripting / File Upload
Academy LMS version 6.1 suffers from an upload vulnerability that could lead to persistent cross site scripting attacks.
- Link
—
” “Mon, 21 Aug 2023
Credit Lite 1.5.4 SQL Injection
Credit Lite version 1.5.4 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 21 Aug 2023
Crypto Currency Tracker (CCT) 9.5 Add Administrator
Crypto Currency Tracker (CCT) versions 9.5 and below suffer from a flaw that allows an administrative account to be added without authentication.
- Link
—
” “Mon, 21 Aug 2023
Fara Melk Estate CMS 1.5.0 Information Disclosure
Fara Melk Estate CMS version 1.5.0 suffers from an information leakage vulnerability.
- Link
—
” “Mon, 21 Aug 2023
Evsanati Radyo 1.0 Shell Upload
Evsanati Radyo version 1.0 suffers from a remote shell upload vulnerability.
- Link
—
” “Mon, 21 Aug 2023
Event Locations CMS 1.0.1 Shell Upload
Event Locations CMS version 1.0.1 suffers from a remote shell upload vulnerability.
- Link
—
” “Mon, 21 Aug 2023
DoorGets CMS 7.0 Information Disclosure
DoorGets CMS version 7.0 suffers from an information leakage vulnerability.
- Link
—
” “Mon, 21 Aug 2023
Emaar Real Estate Agency Directory System 5.7 Shell Upload
Emaar Real Estate Agency Directory System version 5.7 suffers from a remote shell upload vulnerability.
- Link
—
” “Fri, 18 Aug 2023
Cisco ThousandEyes Enterprise Agent Virtual Appliance Arbitrary File Modification
Cisco ThousandEyes Enterprise Agent Virtual Appliance version thousandeyes-va-64-18.04 0.218 suffers from an unpatched vulnerability in sudoedit, allowed by sudo configuration, which permits a low-privilege user to modify arbitrary files as root and subsequently execute arbitrary commands as root.
- Link
—
” “Fri, 18 Aug 2023

Cisco ThousandEyes Enterprise Agent Virtual Appliance Privilege Escalation
Cisco ThousandEyes Enterprise Agent Virtual Appliance version thousandeyes-va-64-18.04 0.218 has an insecure sudo configuration which permits a low-privilege user to run arbitrary commands as root via the tcpdump command without a password.
- Link
—
” “Fri, 18 Aug 2023
Cisco ThousandEyes Enterprise Agent Virtual Appliance Arbitrary File Read
Cisco ThousandEyes Enterprise Agent Virtual Appliance version thousandeyes-va-64-18.04 0.218 has an insecure sudo configuration which permits a low-privilege user to read root-only files via the dig command without a password.
- Link
—
” “Fri, 18 Aug 2023
Chrome IPCZ FragmentDescriptors Missing Validation
Chrome IPCZ FragmentDescriptors are not validated allowing for an out-of-bounds crash condition.
- Link
—
” “Thu, 17 Aug 2023
Greenshot 1.3.274 Deserialization / Command Execution
There exists a .NET deserialization vulnerability in Greenshot versions 1.3.274 and below. The deserialization allows the execution of commands when a user opens a Greenshot file. The commands execute under the same permissions as the Greenshot service. Typically, it is the logged in user.
- Link
—
” “Thu, 17 Aug 2023
Maltrail 0.53 Unauthenticated Command Injection
Maltrail is a malicious traffic detection system, utilizing publicly available blacklists containing malicious and/or generally suspicious trails. Maltrail versions below 0.54 suffer from a command injection vulnerability. The subprocess.check_output function in mailtrail/core/http.py contains a command injection vulnerability in the params.get(”username”) parameter. An attacker can exploit this vulnerability by injecting arbitrary OS commands into the username parameter. The injected commands will be executed with the privileges of the running process. This vulnerability can be exploited remotely without authentication. Successfully tested against Maltrail versions 0.52 and 0.53.
- Link
—
” “Wed, 16 Aug 2023
AudioCodes VoIP Phones Hardcoded Key
The AudioCodes VoIP phones can be managed centrally, whereby configuration files are provided and requested by the phones at a central location. These configuration files can also be provided in encrypted form. This is intended to protect sensitive information within the configuration files from unauthorized access. Due to the use of a hardcoded cryptographic key, an attacker is able to decrypt encrypted configuration files and retrieve sensitive information. Firmware versions greater than or equal to 3.4.8.M4 are affected.
- Link
—
” “Wed, 16 Aug 2023
AudioCodes VoIP Phones Hardcoded Key
The AudioCodes VoIP phones store sensitive information, e.g. credentials and passwords, in encrypted form in their configuration files. These encrypted values can also be automatically configured, e.g. via the ”One Voice Operation Center” or other central device management solutions. Due to the use of a hardcoded cryptographic key, an attacker with access to these configuration files is able to decrypt the encrypted values and retrieve sensitive information, e.g. the device root password. Firmware versions greater than or equal to 3.4.8.M4 are affected.
- Link
—
” “Wed, 16 Aug 2023
AudioCodes VoIP Phones Insufficient Firmware Validation
AudioCodes VoIP Phones with firmware versions greater than or equal to 3.4.4.1000 have been found to have validation of firmware images that only consists of simple checksum checks for different firmware components.
- Link
—

” “Wed, 16 Aug 2023
Hyip Rio 2.1 Cross Site Scripting / File Upload
Hyip Rio version 2.1 suffers from an arbitrary file upload vulnerability that can be leveraged to commit cross site scripting attacks.
- Link
—
” “Wed, 16 Aug 2023
ExcessWeb And Network CMS 4.0 Database Disclosure
ExcessWeb and Network CMS version 4.0 suffers from a database disclosure vulnerability.
- Link
—
” “Wed, 16 Aug 2023
Evsanati Radyo 1.0 Insecure Settings
Evsanati Radyo version 1.0 suffers from an ignored default credential vulnerability.
- Link
—
” “Wed, 16 Aug 2023
Event Locations CMS 1.0.1 Cross Site Scripting
Event Locations CMS version 1.0.1 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 16 Aug 2023
Erim Upload 4 Database Disclosure
Erim Upload version 4 suffers from a database disclosure vulnerability.
- Link
—
” “Wed, 16 Aug 2023
E-partenaire LMS 1.0.0 Cross Site Scripting
E-partenaire LMS version 1.0.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 16 Aug 2023
EMH CMS 0.1 Cross Site Scripting
EMH CMS version 0.1 suffers from a cross site scripting vulnerability.
- Link
—
”

0-Day

“Mon, 21 Aug 2023
ZDI-23-1158: McAfee Safe Connect VPN Uncontrolled Search Path Element Local Privilege Escalation Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1157: Advantech R-SeeNet device_status Local File Inclusion Privilege Escalation Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1156: Advantech R-SeeNet Use Of Hard-Coded Credentials Authentication Bypass Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1155: SonicWALL GMS Virtual Appliance HttpDigestAuthenticator Authentication Bypass Vulnerability
- Link
—
” “Mon, 21 Aug 2023

ZDI-23-1154: SonicWALL GMS Virtual Appliance Syslog Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1153: 3CX Uncontrolled Search Path Local Privilege Escalation Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!

Zum Youtube Video

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2023-08-21	Hôpital municipal Sfânta Treime de Chișinău	[MDA]	Link
2023-08-21	Le Centre Public d'Action Sociale (CPAS) de Charleroi	[BEL]	Link
2023-08-20	Kansai Nerolac Ltd.	[IND]	Link
2023-08-20	Singing River Health System	[USA]	Link
2023-08-18	Energy One Limited	[AUS]	Link
2023-08-17	Poste Italiane	[ITA]	Link
2023-08-17	La mairie de Sartrouville	[FRA]	Link
2023-08-16	Le consortium de bonification de l'Emilia Centrale	[ITA]	Link
2023-08-15	Cleveland City Schools	[USA]	Link
2023-08-14	Clorox	[USA]	Link
2023-08-14	Prince George's County Public Schools	[USA]	Link
2023-08-13	Swan Retail	[GBR]	Link
2023-08-13	Verlagsgruppe in München	[DEU]	Link
2023-08-11	Neogy	[ITA]	Link
2023-08-11	Freeport-McMoRan Inc.	[USA]	Link
2023-08-09	Rapattoni	[USA]	Link
2023-08-08	Fondation de Verdeil	[CHE]	Link
2023-08-07	Centre médical Mayanei Hayeshua	[ISR]	Link
2023-08-07	Oniris	[FRA]	Link
2023-08-06	Le Service de Santé de Madeira (Sesaram)	[PRT]	Link
2023-08-04	Trinkwasserverband (TWV) Stader Land	[DEU]	Link
2023-08-03	Prospect Medical Holdings	[USA]	Link
2023-08-03	Commission des services électriques de Montréal (CSEM)	[CAN]	Link
2023-08-02	BPP	[GBR]	Link
2023-08-02	Joyson Safety Systems	[DEU]	Link
2023-08-02	L'Association du Barreau Fédéral Allemand (BRAK)	[DEU]	Link
2023-08-01	Programme de Soins Médicaux Intégrés (PAMI)	[ARG]	Link
2023-08-01	Eastern Connecticut Health Network (ECHN) et Waterbury HEALTH	[USA]	Link
2023-08-01	NOIRLab	[USA]	Link

Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-18	[Softverg Co., Ltd.]	noescape	Link
2023-08-13	[FYTISA Industrial Felts and FabricsSL]	noescape	Link
2023-08-13	[Infuance Communication Inc]	noescape	Link
2023-08-21	[Pierce College]	rhysida	Link
2023-08-21	[Department of Defence South African (DARPA)]	snatch	Link
2023-08-21	[apdparcel.com.au]	lockbit3	Link
2023-08-21	[TRIUNE TECHNOFAB PRIVATE LIMITED WAS HACKED]	alphv	Link
2023-08-21	[I&G Broker House]	ransomed	Link
2023-08-21	[A1 Data Provider]	ransomed	Link
2023-08-21	[Department of Defence South African]	snatch	Link
2023-08-21	[Davidoff Hutcher & Citron]	alphv	Link
2023-08-21	[Seiko Group Corporation]	alphv	Link
2023-08-20	[stockwellharris.com]	lockbit3	Link
2023-08-20	[hallbergengineering.com]	lockbit3	Link
2023-08-20	[cloudtopoffice.com]	lockbit3	Link
2023-08-20	[equip-reuse.com]	lockbit3	Link
2023-08-20	[cochraninc.com]	lockbit3	Link
2023-08-19	[Novi Pazar put ad]	medusa	Link
2023-08-19	[The International Civil Defense Organization]	medusa	Link
2023-08-19	[Sartrouville France]	medusa	Link
2023-08-19	[goldmedalbakery]	cuba	Link
2023-08-19	[s3groupltd.com]	lockbit3	Link
2023-08-19	[macuspana.gob.mx]	lockbit3	Link
2023-08-19	[phitoformulas.com.br]	lockbit3	Link
2023-08-18	[ABS Auto Auctions]	play	Link
2023-08-18	[DSA Law Pty Ltd]	play	Link
2023-08-18	[Miami Management]	play	Link
2023-08-18	[BTC Power]	play	Link
2023-08-18	[Stanford Transportation Inc]	play	Link
2023-08-18	[Bolton Group]	play	Link
2023-08-18	[Legends Limousine]	play	Link
2023-08-18	[Oneonline]	play	Link
2023-08-18	[purever.com]	lockbit3	Link
2023-08-18	[neolife.com]	lockbit3	Link
2023-08-09	[mitchcointernational.com]	lockbit3	Link
2023-08-15	[tedpella.com]	lockbit3	Link
2023-08-11	[au Domain Administration Ltd]	noescape	Link
2023-08-11	[Contact 121 Pty Ltd]	noescape	Link
2023-08-17	[umchealth.com]	lockbit3	Link
2023-08-17	[sgl.co.th]	lockbit3	Link
2023-08-17	[Agriloja.pt demo-leak]	everest	Link
2023-08-17	[RIMSS]	akira	Link
2023-08-17	[SFJAZZ.ORG]	lockbit3	Link
2023-08-17	[mybps.us]	lockbit3	Link
2023-08-17	[kriegerklatt.com]	lockbit3	Link
2023-08-17	[ALLIANCE]	blackbasta	Link
2023-08-17	[DEUTSCHELEASING]	blackbasta	Link
2023-08-17	[VDVEN]	blackbasta	Link
2023-08-17	[SYNQUESTLABS]	blackbasta	Link
2023-08-17	[TWINTOWER]	blackbasta	Link
2023-08-17	[Camino Nuevo CharterAcademy]	akira	Link
2023-08-17	[Smart-swgcrc.org]	lockbit3	Link
2023-08-17	[The Clifton Public Schools]	akira	Link
2023-08-17	[MBO-PPS.COM]	clop	Link
2023-08-17	[MBOAMERICA.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-17	[KOMORI.COM]	clop	Link
2023-08-16	[Dillon Supply]	metaencryptor	Link
2023-08-16	[Epicure]	metaencryptor	Link
2023-08-16	[Coswell]	metaencryptor	Link
2023-08-16	[BOB Automotive Group]	metaencryptor	Link
2023-08-16	[Seoul Semiconductor]	metaencryptor	Link
2023-08-16	[Kraiburg Austria GmbH]	metaencryptor	Link
2023-08-16	[Autohaus Ebert GmbH]	metaencryptor	Link
2023-08-16	[CVO Antwerpen]	metaencryptor	Link
2023-08-16	[ICON Creative Studio]	metaencryptor	Link
2023-08-16	[Heilmann Gruppe]	metaencryptor	Link
2023-08-16	[Schwälbchen Molkerei AG]	metaencryptor	Link
2023-08-16	[Münchner Verlagsgruppe GmbH]	metaencryptor	Link
2023-08-16	[Cequint]	akira	Link
2023-08-16	[Tally Energy Services]	akira	Link
2023-08-16	[CORDELLCORDELL]	alphv	Link
2023-08-16	[Municipality of Ferrara]	rhysida	Link
2023-08-16	[Hemmink]	incransom	Link
2023-08-16	[ToyotaLift Northeast]	8base	Link
2023-08-09	[FTRIA CO. LTD]	noescape	Link
2023-08-15	[Recaro]	alphv	Link
2023-08-15	[Postel SpA]	medusa	Link
2023-08-15	[ABA Research - Business Information 2]	alphv	Link
2023-08-15	[Keystone Insurance Services]	8base	Link
2023-08-15	[ANS]	8base	Link
2023-08-15	[Aspect Structural Engineers]	8base	Link
2023-08-08	[Fondation De Verdeil]	noescape	Link
2023-08-14	[Freeport-McMoran - NYSE: FCX]	alphv	Link
2023-08-14	[jhillburn.com]	lockbit3	Link
2023-08-14	[qbcqatar.com.qa]	lockbit3	Link
2023-08-07	[John L Lowery & Associates]	noescape	Link
2023-08-07	[Federal Bar Association]	noescape	Link
2023-08-14	[leecorpinc.com]	lockbit3	Link
2023-08-14	[econsult.com]	lockbit3	Link
2023-08-14	[Saint Xavier University]	alphv	Link
2023-08-14	[Agriloja.pt]	everest	Link
2023-08-14	[CB Energy Australlia]	medusa	Link
2023-08-14	[Borets (Levare.com)]	medusa	Link
2023-08-13	[majan.com]	lockbit3	Link
2023-08-13	[luterkort.se]	lockbit3	Link
2023-08-13	[difccourts.ae]	lockbit3	Link
2023-08-13	[zaun.co.uk]	lockbit3	Link
2023-08-13	[roxcel.com.tr]	lockbit3	Link
2023-08-13	[meaf.com]	lockbit3	Link
2023-08-13	[stmarysschool.co.za]	lockbit3	Link
2023-08-13	[rappenglitz.de]	lockbit3	Link
2023-08-13	[siampremier.co.th]	lockbit3	Link
2023-08-12	[National Institute of Social Services for Retirees and Pensioners]	rhysida	Link
2023-08-12	[Armortex]	bianlian	Link
2023-08-12	[arganoInterRel]	alphv	Link
2023-08-11	[Rite Technology]	akira	Link
2023-08-11	[zain.com]	lockbit3	Link
2023-08-10	[Top Light]	play	Link
2023-08-10	[Algorry Zappia & Associates]	play	Link
2023-08-10	[EAI]	play	Link
2023-08-10	[The Belt Railway Company of Chicago]	akira	Link
2023-08-10	[Optimum Technology]	akira	Link
2023-08-10	[Boson]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-10	[Stockdale Podiatry]	8base	Link
2023-08-09	[oneatlas.com]	lockbit3	Link
2023-08-05	[Lower Yukon School District]	noescape	Link
2023-08-06	[Thermenhotel Stoiser]	incransom	Link
2023-08-09	[el-cerrito.org]	lockbit3	Link
2023-08-09	[fashions-uk.com]	lockbit3	Link
2023-08-09	[cbcstjohns.co.za]	lockbit3	Link
2023-08-09	[octoso.de]	lockbit3	Link
2023-08-09	[ricks-motorcycles.com]	lockbit3	Link
2023-08-09	[janus-engineering.com]	lockbit3	Link
2023-08-09	[csem.qc.ca]	lockbit3	Link
2023-08-09	[asfcustomers.com]	lockbit3	Link
2023-08-09	[sekuro.com.tr]	lockbit3	Link
2023-08-09	[TIMECO]	akira	Link
2023-08-09	[chula.ac.th]	lockbit3	Link
2023-08-09	[etisaleg.com]	lockbit3	Link
2023-08-09	[2plan.com]	lockbit3	Link
2023-08-08	[Sabalan Azmayesh]	arvinclub	Link
2023-08-09	[Optimum Health Solutions]	rhysida	Link
2023-08-09	[unitycouncil.org]	lockbit3	Link
2023-08-09	[independenceia.org]	lockbit3	Link
2023-08-09	[www.finitia.net]	abyss	Link
2023-08-09	[Ramtha]	rhysida	Link
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	Link
2023-08-08	[ZESA Holdings]	everest	Link
2023-08-08	[Magic Micro Computers]	alphv	Link
2023-08-08	[Emerson School District]	medusa	Link
2023-08-08	[CH informatica]	8base	Link
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	Link
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	Link
2023-08-07	[Papel Prensa SA]	akira	Link
2023-08-01	[Kreacta]	noescape	Link
2023-08-07	[Parsian Bitumen]	arvinclub	Link
2023-08-07	[varian.com]	lockbit3	Link
2023-08-06	[Delaney Browne Recruitment]	8base	Link
2023-08-06	[IBL]	alphv	Link
2023-08-05	[Draje food industrial group]	arvinclub	Link
2023-08-06	[Oregon Sports Medicine]	8base	Link
2023-08-06	[premierbpo.com]	alphv	Link
2023-08-06	[SatCom Marketing]	8base	Link
2023-08-05	[Rayden Solicitors]	alphv	Link
2023-08-05	[haynesintl.com]	lockbit3	Link
2023-08-05	[Kovair Software Data Leak]	everest	Link
2023-08-05	[Henlaw]	alphv	Link
2023-08-04	[mipe.com]	lockbit3	Link
2023-08-04	[armortex.com]	lockbit3	Link
2023-08-04	[iqcontrols.com]	lockbit3	Link
2023-08-04	[scottevest.com]	lockbit3	Link
2023-08-04	[atser.com]	lockbit3	Link
2023-08-04	[Galicia en Goles]	alphv	Link
2023-08-04	[tetco.com]	lockbit3	Link
2023-08-04	[SBS Construction]	alphv	Link
2023-08-04	[Koury Engineering]	akira	Link
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information]	alphv	Link
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	Link
2023-08-04	[seaside-kish co]	arvinclub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-04	[Studio Domaine LLC]	nokoyawa	Link
2023-08-04	[THECHANGE]	alphv	Link
2023-08-04	[Ofimedic]	alphv	Link
2023-08-04	[Abatti Companies - Press Release]	monti	Link
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link
2023-08-02	[fec-corp.com]	lockbit3	Link
2023-08-02	[bestmotel.de]	lockbit3	Link
2023-08-02	[Tempur Sealy International]	alphv	Link
2023-08-02	[constructioncrd.com]	lockbit3	Link
2023-08-02	[Helen F. Dalton Lawyers]	alphv	Link
2023-08-02	[TGRWA]	akira	Link
2023-08-02	[Guido]	akira	Link
2023-08-02	[Bickel & Brewer - Press Release]	monti	Link
2023-08-02	[SHERMAN.EDU]	clop	Link
2023-08-02	[COSI]	karakurt	Link
2023-08-02	[unicorpusa.com]	lockbit3	Link
2023-08-01	[Garage Living, The Dispenser USA]	play	Link
2023-08-01	[Aapd]	play	Link
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	Link
2023-08-01	[DAL-TECH Engineering]	play	Link
2023-08-01	[Coral Resort]	play	Link
2023-08-01	[Professionnel France]	play	Link
2023-08-01	[ACTIVA Group]	play	Link
2023-08-01	[Aquatlantis]	play	Link
2023-08-01	[Kogetsu]	mallox	Link
2023-08-01	[Parathon by JDA eHealth Systems]	akira	Link
2023-08-01	[KIMCO Staffing Service]	alphv	Link
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	Link
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	8base	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.