Cybersecurity Morgenreport

Ausgabe: 20230919

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

Qnap-Updates schließen hochriskante Lücke
Qnap hat aktualisierte Betriebssysteme veröffentlicht. Die neuen QTS-, QuTS-hero- und QuTScloud-Releases schließen teils hochriskante Lücken.
- Link

Anonymisierendes Linux: Kritische libWebP-Lücke in Tails 5.17.1 geschlossen
Die Maintainer des anonymisierenden Linux Tails für den USB-Stick haben in Version 5.17.1 die bereits angegriffene, kritische libWebP-Lücke geschlossen.
- Link

Jetzt patchen! Sicherheitslösungen von Fortinet als Sicherheitsrisiko
Mehrere Produkte von Fortinet sind verwundbar. Sicherheitsupdates schaffen Abhilfe.
- Link

Management-Controller Lenovo XCC: Angreifer können Passwörter manipulieren
Der Computerhersteller Lenovo hat in XClarity Controller mehrere Sicherheitslücken geschlossen.
- Link

Sicherheitsupdates: Schadcode-Schlupflöcher in Foxit PDF geschlossen
Angreifer können Windows-Systeme mit Foxit PDF Editor oder Foxit PDF Reader attackieren.
- Link

Notfallpatch sichert Firefox und Thunderbird gegen Attacken ab
Mozilla hat in seinen Webbrowsern und seinem Mailclient eine Sicherheitslücke geschlossen, die Angreifer bereits ausnutzen.
- Link

Patchday: Angriffe mittels präparierter PDF-Dateien auf Adobe Acrobat
Adobe hat in Acrobat und Reader, Connect und Experience Manager mehrere Sicherheitslücken geschlossen.
- Link

Patchday: Angreifer attackieren unter anderem Microsoft Word
Microsoft hat für Windows & Co. wichtige Sicherheitsupdates veröffentlicht. Zwei Lücken nutzen Angreifer bereits aus.
- Link

Patchday: SAP schließt kritische Datenleak-Lücke in BusinessObjects
Es sind wichtige Sicherheitsupdates für SAP-Software erschienen. Admins sollten zeitnah handeln.
- Link

Jetzt patchen! Attacken auf kritische Schadcode-Lücke in Chrome naheliegend
Google warnt vor Exploitcode für eine Schwachstelle in Chrome. Eine abgesicherte Version des Webbrowsers ist verfügbar.
- Link

Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-39143	0.921370000	0.985870000	Link
CVE-2023-38035	0.973270000	0.998150000	Link
CVE-2023-3519	0.911990000	0.984970000	Link
CVE-2023-35078	0.965240000	0.994270000	Link
CVE-2023-34362	0.936790000	0.987890000	Link
CVE-2023-33246	0.971460000	0.997030000	Link
CVE-2023-32315	0.973180000	0.998100000	Link
CVE-2023-28771	0.926550000	0.986480000	Link
CVE-2023-28121	0.937820000	0.988020000	Link
CVE-2023-27524	0.964400000	0.993910000	Link
CVE-2023-27372	0.970960000	0.996750000	Link
CVE-2023-27350	0.970860000	0.996710000	Link
CVE-2023-26469	0.910820000	0.984840000	Link
CVE-2023-26360	0.904380000	0.984210000	Link
CVE-2023-25717	0.965660000	0.994500000	Link
CVE-2023-25194	0.924830000	0.986240000	Link
CVE-2023-24489	0.974500000	0.999190000	Link
CVE-2023-21839	0.960800000	0.992730000	Link
CVE-2023-21823	0.907830000	0.984540000	Link
CVE-2023-21554	0.961360000	0.992870000	Link
CVE-2023-20887	0.954150000	0.991120000	Link
CVE-2023-0669	0.965780000	0.994530000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 18 Sep 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit

Administratorrechten auszuführen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Mon, 18 Sep 2023
[NEU] [hoch] HPE OneView: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in der HPE OneView API ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen
Ein entfernter, authetisierter oder anonymer Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, seine Rechte zu erweitern und die Domäne vollständig zu kompromittieren.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [kritisch] Samba: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Informationen offenzulegen, um einen Denial of Service Zustand herbeizuführen, um Rechte zu erlangen und um beliebigen Code mit Root-Rechten auszuführen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, einen Denial of Service Zustand zu verursachen oder seine Rechte zu erweitern.
- Link
—
Mon, 18 Sep 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
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Samba: Mehrere Schwachstellen
Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um Dateien zu manipulieren und Informationen offenzulegen.
- Link
—
Mon, 18 Sep 2023
[UPDATE] [hoch] Google Android Patchday Mai 2023

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand auszulösen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] win.rar WinRAR: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in win.rar WinRAR ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann diese Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen und Cross-Site-Scripting (XSS)-Angriffe durchzuführen.
- Link

—

Mon, 18 Sep 2023
[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 18 Sep 2023
[NEU] [hoch] QNAP NAS: Mehrere Schwachstellen
Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in QNAP NAS ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.
- Link

—

Fri, 15 Sep 2023
[UPDATE] [hoch] Mozilla Firefox: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 15 Sep 2023
[NEU] [hoch] IBM Operational Decision Manager: Mehrere Schwachstellen
Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in IBM Operational Decision Manager ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.
- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/18/2023	[RHEL 7 : firefox (RHSA-2023:5197)]	critical
9/18/2023	[RHEL 7 : thunderbird (RHSA-2023:5191)]	critical
9/18/2023	[RHEL 8 : thunderbird (RHSA-2023:5202)]	critical
9/18/2023	[RHEL 9 : firefox (RHSA-2023:5200)]	critical
9/18/2023	[RHEL 8 : firefox (RHSA-2023:5198)]	critical
9/18/2023	[RHEL 8 : libwebp (RHSA-2023:5190)]	critical
9/18/2023	[RHEL 8 : thunderbird (RHSA-2023:5201)]	critical
9/18/2023	[RHEL 8 : thunderbird (RHSA-2023:5185)]	critical
9/18/2023	[RHEL 8 : thunderbird (RHSA-2023:5188)]	critical
9/18/2023	[RHEL 8 : thunderbird (RHSA-2023:5186)]	critical
9/18/2023	[RHEL 8 : firefox (RHSA-2023:5183)]	critical
9/18/2023	[RHEL 8 : libwebp (RHSA-2023:5189)]	critical
9/18/2023	[Oracle Linux 9 : istio (ELSA-2023-12771)]	critical
9/18/2023	[Oracle Linux 7 / 8 : Unbreakable Enterprise kernel (ELSA-2023-12803)]	critical
9/18/2023	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2023-12800)]	critical
9/18/2023	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2023-12799)]	critical
9/18/2023	[Oracle Linux 8 : Unbreakable Enterprise kernel-container (ELSA-2023-12801)]	critical
9/18/2023	[Oracle Linux 7 : Unbreakable Enterprise kernel-container (ELSA-2023-12802)]	critical
9/18/2023	[Oracle Linux 8 / 9 : Unbreakable Enterprise kernel (ELSA-2023-12798)]	critical
9/18/2023	[Slackware Linux 14.1 / 14.2 / 15.0 / current netatalk Vulnerability (SSA:2023-261-01)]	critical
9/18/2023	[GitLab 0.0 < 16.2.7 / 16.3 < 16.3.4 (CVE-2023-4998)]	critical
9/18/2023	[Ubuntu 22.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6339-4)]	critical
9/18/2023	[Debian DLA-3570-1 : libwebp - LTS security update]	critical
9/18/2023	[Fedora 38 : giflib (2023-1b5f6f4eb2)]	critical
9/18/2023	[RHEL 8 : frr (RHSA-2023:5196)]	high
9/18/2023	[Ubuntu 20.04 LTS : c-ares vulnerability (USN-6376-1)]	high
9/18/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Django vulnerability (USN-6378-1)]	high
9/18/2023	[Ubuntu 20.04 LTS : vsftpd vulnerability (USN-6379-1)]	high
9/18/2023	[RHEL 9 : frr (RHSA-2023:5194)]	high
9/18/2023	[RHEL 8 : frr (RHSA-2023:5195)]	high
9/18/2023	[Oracle Linux 9 : thunderbird (ELSA-2023-4955)]	high
9/18/2023	[Oracle Linux 8 : thunderbird (ELSA-2023-4954)]	high
9/18/2023	[Ubuntu 16.04 ESM / 18.04 ESM : GNU binutils vulnerabilities (USN-6381-1)]	high
9/18/2023	[Wago CODESYS V3 Out-of-bounds Write (CVE-2022-47379)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47390)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47383)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47384)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47381)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47385)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47386)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47382)]	high

Datum	Schwachstelle	Bewertung
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47387)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47388)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47380)]	high
9/18/2023	[Wago CODESYS V3 Improper Input Validation (CVE-2022-47391)]	high
9/18/2023	[Wago CODESYS V3 Stack-based Buffer Overflow (CVE-2022-47389)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Mon, 18 Sep 2023
Atos Unify OpenScape Code Execution / Missing Authentication
Atos Unify OpenScape Session Border Controller, Atos Unify OpenScape Branch, and Atos Unify OpenScape BCF suffer from remote code execution and missing authentication vulnerabilities. Atos OpenScape SBC versions before 10 R3.3.0, Branch version 10 versions before R3.3.0, and BCF version 10 versions before 10 R10.10.0 are affected.
- Link
—
” “Mon, 18 Sep 2023
PTC - Codebeamer Cross Site Scripting
PTC - Codebeamer versions 22.10-SP7 and below, 22.04-SP5 and below, and 21.09-SP13 and below suffer from a cross site scripting vulnerability.
- Link
—
” “Mon, 18 Sep 2023
Ivanti Avalanche MDM Buffer Overflow
This Metasploit module exploits a buffer overflow condition in Ivanti Avalanche MDM versions prior to 6.4.1. An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in arbitrary code execution with the NT/AUTHORITY SYSTEM permissions. This vulnerability occurs during the processing of 3/5/8/100/101/102 item data types. The program tries to copy the item data using qmemcopy to a fixed size data buffer on stack. Upon successful exploitation the attacker gains full access to the target system. This vulnerability has been tested against Ivanti Avalanche MDM version 6.4.0.0 on Windows 10.
- Link
—
” “Mon, 18 Sep 2023
Razer Synapse Race Condition / DLL Hijacking
Razer Synapse versions before 3.8.0428.042117 (20230601) suffer from multiple vulnerabilities. Due to an unsafe installation path, improper privilege management, and a time-of-check time-of-use race condition, the associated system service ”Razer Synapse Service” is vulnerable to DLL hijacking. As a result, local Windows users can abuse the Razer driver installer to obtain administrative privileges on Windows.
- Link
—
” “Mon, 18 Sep 2023
KPOT Stealer CMS 2.0 Directory Traversal
KPOT Stealer CMS 2.0 suffers from a directory traversal vulnerability.
- Link
—
” “Mon, 18 Sep 2023
KPK CMS 1.0 SQL Injection
KPK CMS version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Mon, 18 Sep 2023
Karenderia MRS 5.3 Directory Traversal
Karenderia MRS version 5.3 suffers from a directory traversal vulnerability.
- Link
—
” “Fri, 15 Sep 2023
Academy LMS 6.2 SQL Injection
Academy LMS version 6.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Fri, 15 Sep 2023
Academy LMS 6.2 Cross Site Scripting
Academy LMS version 6.2 suffers from a cross site scripting vulnerability.
- Link
—

” “Fri, 15 Sep 2023
Italia Mediasky CMS 2.0 Cross Site Scripting
Italia Mediasky CMS version 2.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Fri, 15 Sep 2023
Italia Mediasky CMS 2.0 Cross Site Request Forgery
Italia Mediasky CMS version 2.0 suffers from a cross site request forgery vulnerability.
- Link
—
” “Fri, 15 Sep 2023
Chrome Read-Only Property Overwrite
Chrome suffers from a read-only property overwrite in TurboFan.
- Link
—
” “Thu, 14 Sep 2023
Windows Common Log File System Driver (clfs.sys) Privilege Escalation
A privilege escalation vulnerability exists in the clfs.sys driver which comes installed by default on Windows 10 21H2, Windows 11 21H2 and Windows Server 20348 operating systems. This Metasploit module exploit makes use to two different kinds of specially crafted .blf files.
- Link
—
” “Thu, 14 Sep 2023
iSmile Soft CMS 0.3.0 Add Administrator
iSmile Soft CMS version 0.3.0 suffers from an add administrator vulnerability.
- Link
—
” “Thu, 14 Sep 2023
islamnt CMS 2.1.0 Add Administrator
islamnt CMS version 2.1.0 suffers from an add administrator vulnerability.
- Link
—
” “Thu, 14 Sep 2023
islamnt CMS 2.1.0 Cross Site Scripting
islamnt CMS version 2.1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 14 Sep 2023
Night Club Booking Software 1.0 Cross Site Scripting
Night Club Booking Software version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 14 Sep 2023
ImgHosting 1.3 Cross Site Scripting
ImgHosting version 1.3 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 13 Sep 2023
Ivanti Sentry Authentication Bypass / Remote Code Execution
This Metasploit module exploits an authentication bypass in Ivanti Sentry which exposes API functionality which allows for code execution in the context of the root user.
- Link
—
” “Wed, 13 Sep 2023
PHP Shopping Cart 4.2 SQL Injection
PHP Shopping Cart version 4.2 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 13 Sep 2023
Fundraising Script 1.0 SQL Injection
Fundraising Script version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 13 Sep 2023

Blood Bank And Donor Management System 2.2 Cross Site Scripting

Blood Bank and Donor Management System version 2.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 13 Sep 2023

Kleeja 1.5.4 Cross Site Scripting

Kleeja version 1.5.4 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 13 Sep 2023

K-LOANS 1.4.5 Insecure Settings

K-LOANS version 1.4.5 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 12 Sep 2023

Online Pizza Ordering System 1.0 Shell Upload

This Metasploit module exploits a vulnerability found in Online Pizza Ordering System version 1.0. By abusing the admin_class.php file, a malicious user can upload a file to the img/ directory without any authentication, which results in arbitrary code execution. The module has been tested successfully on Ubuntu 22.04.

- Link

—

”

0-Day

Die Hacks der Woche

mit Martin Haunschmid

Schlechte Neuigkeiten: LastPass Tresore geknackt? UND: Wie der Microsoft Signing Key verschwand

Zum Youtube Video

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2023-09-14	Auckland Transport	[NZL]	Link
2023-09-12	Un prestataire de Pelmorex Corp.	[CAN]	Link
2023-09-12	IFX Networks	[COL]	Link
2023-09-11	MGM Resorts	[USA]	Link
2023-09-11	Partenaire de moBiel	[DEU]	Link
2023-09-11	Le système d'information judiciaire régional (REJIS) du comté de St. Louis	[USA]	Link
2023-09-11	Zetema Progetto Cultura	[ITA]	Link
2023-09-11	Agence de relations publiques ikp	[AUT]	Link
2023-09-07	Le groupe hospitalier Saint-Vincent à Strasbourg	[FRA]	Link
2023-09-06	L'académie St Augustine à Maidstone	[GBR]	Link
2023-09-06	Comté de Hinds	[USA]	Link
2023-09-06	ORBCOMM	[USA]	Link
2023-09-05	Mairie de Séville	[ESP]	Link
2023-09-05	Financial Services Commission (FSC)	[JAM]	Link
2023-09-05	Decatur Independent School District (DISD)	[USA]	Link
2023-09-05	Thermae 2000	[NLD]	Link
2023-09-04	Maiden Erlegh Trust	[GBR]	Link
2023-09-01	Comitato Elettrotecnico Italiano (CEI)	[ITA]	Link
2023-09-01	Secrétariat de l'environnement et des ressources naturelles (Semarnat)	[MEX]	Link

Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-19	[Hacketts printing services]	knight	Link
2023-09-19	[CEFCO]	snatch	Link
2023-09-19	[ZILLI]	snatch	Link
2023-09-19	[Florida Department of Veterans' Affairs]	snatch	Link
2023-09-17	[CITIZEN company LEAKED]	ragnarlocker	Link
2023-09-18	[First Line]	play	Link
2023-09-18	[Rea Magnet Wire]	play	Link
2023-09-18	[RTA]	play	Link
2023-09-18	[TSC]	play	Link
2023-09-18	[PASCHAL - Werk G Maier]	play	Link
2023-09-18	[Vucke]	play	Link
2023-09-18	[Elemetal]	incransom	Link
2023-09-18	[Glovis America]	akira	Link
2023-09-18	[Fuji Seal International (US branch)]	akira	Link
2023-09-18	[Hoteles Xcaret]	blackbyte	Link
2023-09-18	[Agriloja.pt Full Leak]	everest	Link
2023-09-18	[Dustin J Will LCC / Dustin J Will Sole MBR]	knight	Link
2023-09-18	[Lopez & Associates Inc]	knight	Link
2023-09-18	[Auckland Transport]	medusa	Link
2023-09-18	[Araújo e Policastro Advogados]	8base	Link
2023-09-17	[Announcement: Retail House going to be LEAKED]	ragnarlocker	Link
2023-09-17	[Delta Group]	8base	Link
2023-09-16	[TransTerra]	cyphbit	Link
2023-09-16	[Marston Domsel]	cyphbit	Link
2023-09-16	[tuvsud.com]	lockbit3	Link
2023-09-16	[perfectlaw.com]	lockbit3	Link
2023-09-16	[beamconstruction.com]	lockbit3	Link
2023-09-16	[scottpartners.com]	lockbit3	Link
2023-09-16	[eljayoil.com]	lockbit3	Link
2023-09-16	[dasholding.ae]	lockbit3	Link
2023-09-16	[faithfamilyacademy.org]	lockbit3	Link
2023-09-16	[syntech.com.sg]	lockbit3	Link
2023-09-16	[piramidal.com.br]	lockbit3	Link
2023-09-16	[tlip2.com]	lockbit3	Link
2023-09-16	[energyinsight.co.za]	lockbit3	Link
2023-09-16	[mehmetceylanyapi.com.tr]	lockbit3	Link
2023-09-16	[aeroportlleida.cat]	lockbit3	Link
2023-09-16	[lamaisonmercier.com]	lockbit3	Link
2023-09-16	[neolaser.es]	lockbit3	Link
2023-09-16	[commercialfluidpower.com]	lockbit3	Link
2023-09-16	[glat.zapweb.co.il]	lockbit3	Link
2023-09-16	[motsaot.co.il]	lockbit3	Link
2023-09-16	[gsaenz.com.mx]	lockbit3	Link
2023-09-16	[ipsenlogistics.com]	lockbit3	Link
2023-09-16	[Financial Decisions]	alphv	Link
2023-09-15	[Updates: Israel "MYMC"]	ragnarlocker	Link
2023-09-15	[hollandspecial]	alphv	Link
2023-09-15	[pelicanwoodcliff.com]	lockbit3	Link
2023-09-15	[hillsboroughschools.org]	lockbit3	Link
2023-09-15	[Steelforce]	trigona	Link
2023-09-14	[wdgroup.com.my]	threeam	Link
2023-09-14	[pvbfabs.com]	threeam	Link
2023-09-14	[intechims.com]	threeam	Link
2023-09-14	[zero-pointorganics.com]	threeam	Link
2023-09-14	[visitingphysiciansnetwork.com]	threeam	Link
2023-09-14	[clearwaterlandscape.com]	threeam	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-14	[Statement on MGM Resorts International: Setting the record straight]	alphv	Link
2023-09-14	[etsi.uy]	knight	Link
2023-09-14	[Ja Quith Press Release]	monti	Link
2023-09-14	[East Baking Press Release]	monti	Link
2023-09-14	[American Steel & Aluminum]	akira	Link
2023-09-14	[Waterford Retirement Residence]	cyphbit	Link
2023-09-14	[Shelly Engineering Metal Work]	cyphbit	Link
2023-09-14	[Harmonic Accounting]	cyphbit	Link
2023-09-14	[Imperador S.R.L]	cyphbit	Link
2023-09-14	[Waterford Retirement Residence]	cyphbit	Link
2023-09-14	[Shelly Engineering Metal Work]	cyphbit	Link
2023-09-14	[RSV Centrale Bvba]	cyphbit	Link
2023-09-14	[Soprovise]	cyphbit	Link
2023-09-14	[carthagehospital.com]	lockbit3	Link
2023-09-07	[Fondation Vincent De Paul]	noescape	Link
2023-09-07	[EDUCAL, SA de CV]	noescape	Link
2023-09-13	[Enpos]	stormous	Link
2023-09-13	[clearcreek.org]	lockbit3	Link
2023-09-13	[Financial Services Commission]	blacksuit	Link
2023-09-13	[Cedar Holdings]	trigona	Link
2023-09-13	[Benefit Management INC]	knight	Link
2023-09-13	[Dpc & S]	play	Link
2023-09-13	[Carpet One]	play	Link
2023-09-13	[Markentrainer Werbeagentur, Elwema Automotive]	play	Link
2023-09-13	[Tanachira Group]	knight	Link
2023-09-12	[Accuride]	akira	Link
2023-09-12	[Abbeyfield]	incransom	Link
2023-09-12	[Morgan Smith Industries LLC]	knight	Link
2023-09-12	[Decarie Motors Inc]	knight	Link
2023-09-12	[sinloc.com]	lockbit3	Link
2023-09-12	[M-Extend / MANIP]	alphv	Link
2023-09-12	[Dee Sign]	lorenz	Link
2023-09-12	[Credifiel was hacked and a lot of personal customer and financial information was stolen]	alphv	Link
2023-09-12	[Derrimon Trading was hacked. Critical data of the company and its customers was stolen]	alphv	Link
2023-09-12	[CORTEL Technologies]	qilin	Link
2023-09-11	[Alps Alpine]	blackbyte	Link
2023-09-11	[24/7 Express Logistics (Unpay-Start Leaking)]	ragroup	Link
2023-09-07	[International Joint Commission]	noescape	Link
2023-09-02	[Altmann Dental GmbH & Co KG]	noescape	Link
2023-09-03	[AdSage Technology Co., Ltd.]	noescape	Link
2023-09-11	[deeroaks.com]	lockbit3	Link
2023-09-11	[Cmranallolaw.com]	everest	Link
2023-09-11	[Wardlaw Claims Service]	cactus	Link
2023-09-11	[Levine Bagade Han]	cactus	Link
2023-09-11	[Leekes]	cactus	Link
2023-09-11	[My Insurance Broker]	cactus	Link
2023-09-11	[Unimarketing]	cactus	Link
2023-09-11	[cfsigroup.ca]	lockbit3	Link
2023-09-11	[Wave Hill]	medusa	Link
2023-09-11	[Steripharma]	medusa	Link
2023-09-11	[co.grant.mn.us]	lockbit3	Link
2023-09-11	[KUITS Solicitors]	alphv	Link
2023-09-11	[Ford Covesa]	8base	Link
2023-09-10	[New Venture Escrow]	bianlian	Link
2023-09-10	[BOZOVICH TIMBER PRODUCTS INC]	mallox	Link
2023-09-10	[njsba.com]	abyss	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-10	[Singing River Health System]	rhysida	Link
2023-09-10	[Core Desktop]	rhysida	Link
2023-09-09	[Kirby Risk]	blackbyte	Link
2023-09-09	[airelec.bg]	ransomed	Link
2023-09-09	[pilini.bg]	ransomed	Link
2023-09-09	[kasida.bg]	ransomed	Link
2023-09-09	[proxy-sale.com]	ransomed	Link
2023-09-09	[IT-Center Syd]	rhysida	Link
2023-09-08	[www.northriverco.com]	abyss	Link
2023-09-08	[sd69.org]	lockbit3	Link
2023-09-08	[milbermakris.com]	lockbit3	Link
2023-09-08	[monaco-technologies.com]	lockbit3	Link
2023-09-08	[UNIVERSAL REALTY GROUP]	8base	Link
2023-09-08	[Geo Tek]	cactus	Link
2023-09-08	[hanwha.com]	lockbit3	Link
2023-09-08	[Custom Powder Systems]	cactus	Link
2023-09-08	[JSS Almonds]	cactus	Link
2023-09-08	[atWork Office Furniture]	cactus	Link
2023-09-08	[BRiC Partnership]	cactus	Link
2023-09-08	[PAUL-ALEXANDRE DOICESCO]	qilin	Link
2023-09-08	[WACOAL]	qilin	Link
2023-09-08	[Linktera]	ransomed	Link
2023-09-07	[24/7 Express Logistics]	ragroup	Link
2023-09-07	[FOCUS Business Solutions]	blackbyte	Link
2023-09-07	[Chambersburg Area School District]	blackbyte	Link
2023-09-07	[Pvc-ms]	stormous	Link
2023-09-07	[toua.net]	lockbit3	Link
2023-09-07	[Conselho Superior da Justiça do Trabalho]	8base	Link
2023-09-07	[Sebata Holdings (MICROmega Holdings)]	bianlian	Link
2023-09-07	[TORMAX USA]	cactus	Link
2023-09-07	[West Craft Manufacturing]	cactus	Link
2023-09-07	[Trimaran Capital Partners]	cactus	Link
2023-09-07	[Specialised Management Services]	cactus	Link
2023-09-06	[nobleweb.com]	lockbit3	Link
2023-09-06	[protosign.it]	lockbit3	Link
2023-09-06	[concrejato.com.br]	lockbit3	Link
2023-09-06	[meroso.be]	lockbit3	Link
2023-09-06	[qsoftnet.com]	lockbit3	Link
2023-09-06	[ragasa.com.mx]	lockbit3	Link
2023-09-06	[I Keating Furniture World]	incransom	Link
2023-09-06	[onyx-fire.com]	lockbit3	Link
2023-09-06	[gormanusa.com]	lockbit3	Link
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	Link
2023-09-06	[It4 Solutions Robras]	incransom	Link
2023-09-06	[Smead]	blackbyte	Link
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	Link
2023-09-06	[Ayass BioScience]	alphv	Link
2023-09-06	[Sabre Corporation]	dunghill_leak	Link
2023-09-06	[Energy One]	akira	Link
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	Link
2023-09-06	[Chula Vista Electric (CVE)]	8base	Link
2023-09-05	[Precisely, Winshuttle]	play	Link
2023-09-05	[Kikkerland Design]	play	Link
2023-09-05	[Markentrainer Werbeagentur]	play	Link
2023-09-05	[Master Interiors]	play	Link
2023-09-05	[Bordelon Marine]	play	Link
2023-09-05	[Majestic Spice]	play	Link
2023-09-04	[Infinity Construction Company]	noescape	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-05	[Maxxd Trailers]	cactus	Link
2023-09-05	[MINEMAN Systems]	cactus	Link
2023-09-05	[Promotrans]	cactus	Link
2023-09-05	[Seymours]	cactus	Link
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	Link
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	Link
2023-09-05	[Marfrig Global Foods]	cactus	Link
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	Link
2023-09-05	[Barry Plant LEAK!]	alphv	Link
2023-09-05	[Barsco]	cactus	Link
2023-09-05	[Foroni SPA]	cactus	Link
2023-09-05	[Hornsyld Købmandsgaard]	cactus	Link
2023-09-05	[Lagarde Meregnani]	cactus	Link
2023-09-05	[spmblaw.com]	lockbit3	Link
2023-09-05	[Unimed]	trigona	Link
2023-09-05	[Cyberport]	trigona	Link
2023-09-05	[godbeylaw.com]	lockbit3	Link
2023-09-01	[Firmdale Hotels]	play	Link
2023-09-04	[easydentalcare.us]	ransomed	Link
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
2023-09-04	[makflix.eu]	ransomed	Link
2023-09-04	[nucleus.live]	ransomed	Link
2023-09-04	[wantager.com]	ransomed	Link
2023-09-04	[Zurvita]	ragroup	Link
2023-09-04	[Piex Group]	ragroup	Link
2023-09-04	[Yuxin Automobile Co.Ltd ( )]	ragroup	Link
2023-09-02	[Mulkay Cardiology Consultants]	noescape	Link
2023-09-04	[Balcan]	cactus	Link
2023-09-04	[Barco Uniforms]	cactus	Link
2023-09-04	[Swipe.bg]	ransomed	Link
2023-09-04	[Balmit Bulgaria]	ransomed	Link
2023-09-04	[cdwg.com]	lockbit3	Link
2023-09-04	[Betton France]	medusa	Link
2023-09-04	[Jules B]	medusa	Link
2023-09-04	[VVandA]	8base	Link
2023-09-04	[Prodegest Assessors]	8base	Link
2023-09-04	[Knight Barry Title]	snatch	Link
2023-09-03	[phms.com.au]	ransomed	Link
2023-09-03	[paynesvilleareainsurance.com]	ransomed	Link
2023-09-03	[SKF.com]	ransomed	Link
2023-09-03	[gosslaw.com]	lockbit3	Link
2023-09-03	[marianoshoes.com]	lockbit3	Link
2023-09-03	[Arkopharma]	incransom	Link
2023-09-02	[Taylor University]	moneymessage	Link
2023-09-03	[Riverside Logistics]	moneymessage	Link
2023-09-03	[Estes Design & Manufacturing]	moneymessage	Link
2023-09-03	[Aiphone]	moneymessage	Link
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	rancoz	Link
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	rancoz	Link
2023-09-03	[Newton Media A.S]	alphv	Link
2023-09-03	[Lawsonlundell]	alphv	Link
2023-09-02	[glprop.com]	lockbit3	Link
2023-09-02	[Strata Plan Australia]	alphv	Link
2023-09-02	[TissuPath Australia]	alphv	Link
2023-09-02	[seasonsdarlingharbour.com.au]	lockbit3	Link
2023-09-02	[nerolac.com]	lockbit3	Link
2023-09-02	[ramlowstein.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-09-02	[Barry Plant Real Estate Australia]	alphv	Link
2023-09-02	[sterncoengineers.com]	lockbit3	Link
2023-09-02	[attorneydanwinder.com]	lockbit3	Link
2023-09-02	[designlink.us]	lockbit3	Link
2023-09-02	[gh2.com]	lockbit3	Link
2023-09-02	[DOIT - Canadian IT company allowed leak of its own clients.]	ragnarlocker	Link
2023-09-02	[SKF.com]	everest	Link
2023-09-02	[Powersportsmarketing.com]	everest	Link
2023-09-02	[Statefarm.com]	everest	Link
2023-09-02	[Aban Tether & OK exchange]	arvinclub	Link
2023-09-02	[cc-gorgesardeche.fr]	lockbit3	Link
2023-09-01	[cciamp.com]	lockbit3	Link
2023-09-01	[Templeman Consulting Group Inc]	bianlian	Link
2023-09-01	[vodatech.com.tr]	lockbit3	Link
2023-09-01	[F??????? ?????s]	play	Link
2023-09-01	[Hawaii Health System]	ransomed	Link
2023-09-01	[hamilton-techservices.com]	lockbit3	Link
2023-09-01	[aquinas.qld.edu.au]	lockbit3	Link
2023-09-01	[konkconsulting.com]	lockbit3	Link
2023-09-01	[Piex Group]	ragroup	Link
2023-09-01	[Yuxin Automobile Co.Ltd( )]	ragroup	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.