



Ausgabe: 20230906

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

AVM: Fritzbox-Firmware 7.57 und 7.31 stopfen Sicherheitsleck

AVM hat für zahlreiche Fritzboxen die Firmware 7.57 und 7.31 veröffentlicht. Es handelt sich um Stabilitäts- und Sicherheitsupdates.

- [Link](#)

Jetzt aktualisieren! Proof-of-Concept für kritische VMware-Aria-Lücke

Vergangene Woche hat VMware Updates zum Schließen einer kritischen Sicherheitslücke herausgegeben. Jetzt ist ein Proof-of-Concept verfügbar. Zeit fürs Update!

- [Link](#)

Kritische Lücke in VPN von Securepoint

Updates sollen eine kritische Sicherheitslücke in der VPN-Software von Securepoint schließen, durch die Angreifer ihre Rechte ausweiten können.

- [Link](#)

Acronis: Updates dichten Sicherheitslecks in mehreren Produkten ab

Acronis hat Sicherheitsmeldungen zu insgesamt zwölf Schwachstellen in mehreren Produkten herausgegeben. Updates stehen länger bereit.

- [Link](#)

VMware Tools: Schwachstelle ermöglicht Angreifern unbefugte Aktionen in Gästen

VMware warnt vor einer Sicherheitslücke in VMware Tools. Sie ermöglicht eine Man-in-the-Middle-Attacke auf Gastsysteme.

- [Link](#)

Big Data: Splunk dichtet hochriskante Lücken ab

Die Big-Data-Experten von Splunk haben aktualisierte Software bereitgestellt, die teils hochriskante Schwachstellen in der Analysesoftware ausbessert.

- [Link](#)

Sicherheitsupdates: Schadcode-Attacken auf Aruba-Switches möglich

Verschiedene Switch-Modelle von Aruba sind verwundbar. Abgesicherte Ausgaben von ArubaOS schaffen Abhilfe.

- [Link](#)

Entwickler von Notepad++ ignoriert offensichtlich Sicherheitslücken

Mehrere Sicherheitslücken gefährden den Texteditor Notepad++. Trotz Informationen zu den Lücken und möglichen Fixes steht ein Sicherheitsupdate noch aus.

- [Link](#)

Kritische Sicherheitslücke in VMware Aria Operations for Networks

VMware schließt Sicherheitslücken in Aria Operations for Networks. Eine gilt als kritisch und erlaubt den Zugriff ohne Anmeldung.

- [Link](#)

Webbrowser: Google-Chrome-Update stopft hochriskante Sicherheitslücke

Google bessert im Webbrowser Chrome eine als hochriskant eingestufte Schwachstelle aus.

- [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	0.985740000	Link
CVE-2023-38035	0.918170000	0.985380000	Link
CVE-2023-3519	0.911990000	0.984830000	Link
CVE-2023-35078	0.965240000	0.994200000	Link
CVE-2023-34362	0.936790000	0.987820000	Link
CVE-2023-33246	0.963860000	0.993660000	Link
CVE-2023-32315	0.962160000	0.993110000	Link
CVE-2023-28771	0.917110000	0.985260000	Link
CVE-2023-28121	0.937820000	0.987910000	Link
CVE-2023-27372	0.970600000	0.996540000	Link
CVE-2023-27350	0.970860000	0.996690000	Link
CVE-2023-26469	0.910820000	0.984760000	Link
CVE-2023-26360	0.908440000	0.984490000	Link
CVE-2023-25717	0.965660000	0.994410000	Link
CVE-2023-25194	0.924830000	0.986110000	Link
CVE-2023-24489	0.967300000	0.995080000	Link
CVE-2023-21839	0.960800000	0.992720000	Link
CVE-2023-21823	0.907830000	0.984440000	Link
CVE-2023-21554	0.902620000	0.983980000	Link
CVE-2023-20887	0.960660000	0.992670000	Link
CVE-2023-0669	0.965780000	0.994460000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 05 Sep 2023

[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 05 Sep 2023

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- [Link](#)

Tue, 05 Sep 2023

[NEU] [hoch] MinIO: Mehrere Schwachstellen ermöglichen Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in MinIO ausnutzen, um Informationen offenzulegen.

- [Link](#)

Tue, 05 Sep 2023

[NEU] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- [Link](#)

Tue, 05 Sep 2023

[UPDATE] [hoch] Notepad++: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Notepad++ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 05 Sep 2023

[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Tue, 05 Sep 2023

[UPDATE] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 04 Sep 2023

[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- [Link](#)

Mon, 04 Sep 2023

[UPDATE] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- [Link](#)

Mon, 04 Sep 2023

[NEU] [hoch] vim: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Dateien zu manipulieren oder beliebigen Code auszuführen.

- [Link](#)

Mon, 04 Sep 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen und vertrauliche Informationen offenzulegen.

- [Link](#)

Mon, 04 Sep 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](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

Fri, 01 Sep 2023

[NEU] [hoch] Moxa MXsecurity: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Moxa MXsecurity ausnutzen, um Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen.

- [Link](#)

Fri, 01 Sep 2023

[NEU] [hoch] Acronis Cyber Protect Home Office: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Acronis Cyber Protect Home Office ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel und Oracle Linux ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- [Link](#)

Fri, 01 Sep 2023

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/5/2023	[Fedora 38 : libtommath (2023-69b85312f0)]	critical

Datum	Schwachstelle	Bewertung
9/5/2023	[Dell SupportAssist Multiple Vulnerabilities (DSA-2022-139)]	critical
9/5/2023	[Google Chrome < 116.0.5845.179 Multiple Vulnerabilities]	critical
9/5/2023	[Google Chrome < 116.0.5845.179 Multiple Vulnerabilities]	critical
9/5/2023	[Honeywell (CVE-2023-25178)]	critical
9/4/2023	[Ivanti Avalanche Unauthenticated Stack-based Buffer Overflow (CVE-2023-32560)]	critical
9/4/2023	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.7)]	critical
9/4/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6333-1)]	critical
9/4/2023	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.207)]	critical
9/4/2023	[RHEL 7 / 9 : Red Hat JBoss Web Server 5.7.4 release and (RHSA-2023:4909)]	critical
9/4/2023	[Ubuntu 16.04 ESM / 18.04 ESM : BusyBox vulnerabilities (USN-6335-1)]	critical
9/5/2023	[FreeBSD : Django – multiple vulnerabilities (8fd4f40a-4b7d-11ee-aa2a-080027de9982)]	high
9/5/2023	[Fedora 37 : oggvideotools (2023-154d731f46)]	high
9/5/2023	[Fedora 38 : oggvideotools (2023-cf30e790ce)]	high
9/5/2023	[Fedora 38 : exercism (2023-e82fd2abcb)]	high
9/5/2023	[Fedora 37 : moby-engine (2023-cf3551046d)]	high
9/5/2023	[Fedora 37 : exercism (2023-af2e3d1c18)]	high
9/5/2023	[SUSE SLES15 Security Update : terraform (SUSE-SU-2023:3516-1)]	high
9/5/2023	[RHEL 8 : kernel (RHSA-2023:4962)]	high
9/5/2023	[RHEL 8 : kpatch-patch (RHSA-2023:4967)]	high
9/5/2023	[RHEL 8 : kernel-rt (RHSA-2023:4961)]	high
9/5/2023	[Security Update for .NET 7.0 Core SDK (CVE-2023-38178)]	high
9/5/2023	[Security Update for .NET Core SDK (August 2023)]	high
9/5/2023	[Oracle Linux 7 : thunderbird (ELSA-2023-4945)]	high
9/5/2023	[Oracle Linux 7 : binutils (ELSA-2019-2075)]	high
9/5/2023	[VMware Tools 10.3.x / 11.x / 12.x < 12.3.0 Authentication Bypass (VMSA-2023-0019)]	high
9/5/2023	[Honeywell (CVE-2023-24480)]	high
9/5/2023	[Honeywell (CVE-2023-26597)]	high
9/5/2023	[Honeywell (CVE-2023-25770)]	high
9/4/2023	[ClamAV 1.x < 1.0.2 DoS]	high
9/4/2023	[ClamAV < 0.103.9 / 1.0.x < 1.0.2 / 1.1.x < 1.1.1 DoS]	high
9/4/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 ESM : Docker Registry vulnerabilities (USN-6336-1)]	high
9/4/2023	[RHEL 9 : firefox (RHSA-2023:4958)]	high
9/4/2023	[RHEL 9 : firefox (RHSA-2023:4950)]	high
9/4/2023	[RHEL 8 : firefox (RHSA-2023:4949)]	high
9/4/2023	[RHEL 8 : firefox (RHSA-2023:4952)]	high
9/4/2023	[RHEL 8 : thunderbird (RHSA-2023:4956)]	high
9/4/2023	[RHEL 9 : thunderbird (RHSA-2023:4947)]	high
9/4/2023	[RHEL 8 : thunderbird (RHSA-2023:4948)]	high
9/4/2023	[RHEL 8 : firefox (RHSA-2023:4957)]	high
9/4/2023	[RHEL 8 : thunderbird (RHSA-2023:4946)]	high
9/4/2023	[RHEL 7 : thunderbird (RHSA-2023:4945)]	high
9/4/2023	[RHEL 9 : thunderbird (RHSA-2023:4955)]	high
9/4/2023	[RHEL 8 : firefox (RHSA-2023:4959)]	high
9/4/2023	[RHEL 8 : firefox (RHSA-2023:4951)]	high
9/4/2023	[RHEL 8 : thunderbird (RHSA-2023:4954)]	high
9/4/2023	[Ubuntu 18.04 ESM : Linux kernel (Azure) vulnerabilities (USN-6337-1)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Tue, 05 Sep 2023

WordPress Media Library Assistant 3.09 LFI / Remote Code Execution

WordPress Media Library Assistant plugin versions prior to 3.10 are affected by an unauthenticated remote reference to Imagick() conversion which allows attacker to perform local file inclusion and remote code execution depending on the Imagick configuration on the remote server.

- [Link](#)

” “Tue, 05 Sep 2023

Hikvision Access Control Session Hijacking

Remote attackers can steal valid authentication session identifiers of Hikvision Access Control/Intercom Products. This is possible because a remote attacker can create a session identifier without restrictions. If an attacker requests a session ID at the same time as a valid user, the attacker receives the identical session ID. This session ID is immediately recognized as valid after successful authentication of the correct user.

- [Link](#)

” “Tue, 05 Sep 2023

Internet Radio auna IR-160 SE UIProto DoS / XSS / Missing Authentication

Internet Radio auna IR-160 SE using the UIProto firmware suffers from missing authentication, cross site scripting, and denial of service vulnerabilities.

- [Link](#)

” “Tue, 05 Sep 2023

AtlasVPN Linux Client 1.0.3 IP Leak

Remote disconnect exploit for AtlasVPN Linux client version 1.0.3 that will allow a remote website to extract a client's real IP address.

- [Link](#)

” “Tue, 05 Sep 2023

Freefloat FTP Server 1.0 Buffer Overflow

Freefloat FTP Server version 1.0 suffers from a remote buffer overflow vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

Kingo ROOT 1.5.8 Unquoted Service Path

Kingo ROOT version 1.5.8 suffers from an unquoted service path vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

FileMage Gateway 1.10.9 Local File Inclusion

FileMage Gateway version 1.10.9 suffers from a local file inclusion vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

WEBIGniter 28.7.23 Shell Upload

WEBIGniter version 28.7.23 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

WEBIGniter 28.7.23 Cross Site Scripting

WEBIGniter version 28.7.23 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

DLINK DPH-400SE FRU2.2.15.8 Information Disclosure

DLINK DPH-400SE version FRU2.2.15.8 suffers from an information disclosure vulnerability.

- [Link](#)

” “Tue, 05 Sep 2023

WordPress WP Statistics 13.1.5 SQL Injection

WordPress WP Statistics plugin version 13.1.5 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

Linux 6.4 Use-After-Free / Race Condition

There is a race between mbind() and VMA-locked page faults in the Linux 6.4 kernel, leading to a use-after-free condition.

- [Link](#)

” “Mon, 04 Sep 2023

NVClient 5.0 Stack Buffer Overflow

NVClient version 5.0 suffers from a stack buffer overflow vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

CSZ CMS 1.3.0 Cross Site Scripting

CSZ CMS version 1.3.0 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

” “Mon, 04 Sep 2023

AdminLTE PiHole Broken Access Control

AdminLTE PiHole versions prior to 5.18 suffer from a broken access control vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

Ivanti Avalance Remote Code Execution

Ivanti Avalanche versions prior to 6.4.0.0 suffer from a remote code execution vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

ImpressionTech CMS 1.4 SQL Injection

ImpressionTech CMS version 1.4 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

Impress CMS 1.3.9 Open Redirection

Impress CMS version 1.3.9 suffers from an open redirection vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

ImgHosting 1.3 HTML Injection

ImgHosting version 1.3 suffers from a html injection vulnerability.

- [Link](#)

” “Mon, 04 Sep 2023

Humhub 1.3.13 Shell Upload

Humhub version 1.3.13 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Sat, 02 Sep 2023

Packet Storm New Exploits For August, 2023

This archive contains all of the 305 exploits added to Packet Storm in August, 2023.

- [Link](#)

” “Sat, 02 Sep 2023

Tinycontrol LAN Controller 3 Remote Admin Password Change

Tinycontrol LAN Controller version 3 suffers from an insecure access control allowing an unauthenticated attacker to change accounts passwords and bypass authentication gaining panel control access.

- [Link](#)

” “Sat, 02 Sep 2023

Tinycontrol LAN Controller 3 Remote Credential Extraction

Tinycontrol LAN Controller version 3 suffers from an issue where an unauthenticated attacker can retrieve the controller’s configuration backup file and extract sensitive information that can allow him/her/them to bypass security controls and penetrate the system in its entirety.

- [Link](#)

” “Sat, 02 Sep 2023

Tinycontrol LAN Controller 3 Denial Of Service

Tinycontrol LAN Controller version 3 suffers from an unauthenticated remote denial of service vulnerability. An attacker can issue direct requests to the stm.cgi page to reboot and also reset factory settings on the device.

- [Link](#)

” “Sat, 02 Sep 2023

VMWare Aria Operations For Networks Remote Code Execution

VMWare Aria Operations for Networks (vRealize Network Insight) static SSH key remote code execution proof of concept exploit.

- [Link](#)

”

0-Day

Die Hacks der Woche

mit Martin Haunschmid

Private video

Vorschaubild [Zum Youtube Video](#)

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
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-Gruppe	Webseite
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
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	[Froni 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	[quantinum.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	[gossilaw.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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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.