Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240904

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 11

4 Aktiv ausgenutzte Sicherheitslücken **12**
4.1 Exploits der letzten 5 Tage . . . 12
4.2 0-Days der letzten 5 Tage . . . 16

5 Die Hacks der Woche **17**
5.0.1 Private video . . . 17

6 Cyberangriffe: (Sep) **18**

7 Ransomware-Erpressungen: (Sep) **18**

8 Quellen **19**
8.1 Quellenverzeichnis . . . 19

9 Impressum **20**

1 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

2 Security-News

2.1 Heise - Security-Alert

Zyxel: Mehrere hochriskante Sicherheitslücken in Firewalls

Zyxel warnt vor mehreren Sicherheitslücken in den Firewalls des Unternehmens. Updates stehen bereit, die Lecks abdichten.

- Link

—

VMware Fusion: Update stopft Rechteausweitungslücke

Broadcom schließt mit einem Update eine Sicherheitslücke in VMware Fusion. Angreifer können ihre Rechte dadurch ausweiten.

- Link

—

“Whatsup Gold”: Umgehen der Anmeldung durch kritische Sicherheitslücken möglich

Progress schließt mit aktualisierter Software kritische Sicherheitslücken in der Monitoring-Software “Whatsup Gold”.

- Link

—

Support ausgelaufen: Attacken auf IP-Kamera von Avtech beobachtet

Derzeit attackiert das Corona-Mirai-Botnet die IP-Kamera AVM1203 von Avtech. Die Kamera wird in öffentlichen Einrichtungen und Industrieanlagen verwendet.

- Link

—

BIOS-Update: Angreifer können Secure Boot auf Alienware-Notebooks umgehen

Unter bestimmten Voraussetzungen können Angreifer eine zentrale Schutzfunktion von Dells Alienware-Notebooks umgehen.

- Link

—

Fortra FileCatalyst Workflow: Hintertür macht Angreifer zu Admins

Aufgrund von hartkodierten Zugangsdaten können sich Angreifer weitreichenden Zugriff auf Fortra FileCatalyst Workflow verschaffen.

- Link

—

Sicherheitsupdates: Cisco Switches sind für DoS-Attacken anfällig

Es sind wichtige Sicherheitsupdates für verschiedene Produkte des Netzwerkausrüsters Cisco erscheinen.

- Link

—

Hitachi Ops Center: Attacken auf Hitachi-Speicherinfrastruktur möglich

Hitachi Ops Center Common Services ist unter Linux verwundbar. Eine abgesicherte Version ist erschienen.

- Link

—

Ticketsystem OTRS: Angreifer können unverschlüsselte Passwörter einsehen

Die Entwickler des Open Ticket Request System haben mehrere Sicherheitslücken geschlossen.

- Link

—

Jetzt patchen! Netzwerksoftware Versa Director attackiert

Derzeit nutzen Angreifer eine Schwachstelle in der Virtualisierungs- und Serviceerstellungsplattform Versa Director aus.

- Link

—

3 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.

3.1 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.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-7028	0.936210000	0.991700000	Link
CVE-2023-6895	0.921160000	0.990130000	Link
CVE-2023-6553	0.921020000	0.990110000	Link
CVE-2023-6019	0.918710000	0.989870000	Link
CVE-2023-5360	0.902780000	0.988860000	Link
CVE-2023-52251	0.946410000	0.992920000	Link
CVE-2023-4966	0.970940000	0.998180000	Link
CVE-2023-49103	0.964030000	0.996060000	Link
CVE-2023-48795	0.965330000	0.996450000	Link
CVE-2023-47246	0.959760000	0.995180000	Link
CVE-2023-46805	0.950230000	0.993560000	Link
CVE-2023-46747	0.972260000	0.998640000	Link
CVE-2023-46604	0.968800000	0.997420000	Link
CVE-2023-4542	0.948590000	0.993270000	Link
CVE-2023-43208	0.973970000	0.999380000	Link
CVE-2023-43177	0.961750000	0.995560000	Link
CVE-2023-42793	0.971190000	0.998300000	Link
CVE-2023-41265	0.911110000	0.989390000	Link
CVE-2023-39143	0.940480000	0.992160000	Link
CVE-2023-38205	0.953670000	0.994160000	Link
CVE-2023-38203	0.965830000	0.996600000	Link
CVE-2023-38146	0.920720000	0.990070000	Link
CVE-2023-38035	0.974690000	0.999730000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996860000	Link
CVE-2023-3519	0.965910000	0.996610000	Link
CVE-2023-35082	0.967460000	0.997060000	Link
CVE-2023-35078	0.970450000	0.997960000	Link
CVE-2023-34993	0.973540000	0.999190000	Link
CVE-2023-34960	0.921610000	0.990190000	Link
CVE-2023-34634	0.923140000	0.990340000	Link
CVE-2023-34362	0.970450000	0.997960000	Link
CVE-2023-34039	0.952470000	0.993960000	Link
CVE-2023-3368	0.942130000	0.992340000	Link
CVE-2023-33246	0.967180000	0.996980000	Link
CVE-2023-32315	0.970220000	0.997870000	Link
CVE-2023-30625	0.953610000	0.994150000	Link
CVE-2023-30013	0.965950000	0.996630000	Link
CVE-2023-29300	0.969240000	0.997570000	Link
CVE-2023-29298	0.941540000	0.992290000	Link
CVE-2023-28432	0.907350000	0.989140000	Link
CVE-2023-28343	0.933130000	0.991430000	Link
CVE-2023-28121	0.919520000	0.989950000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.973470000	0.999170000	Link
CVE-2023-27350	0.968480000	0.997320000	Link
CVE-2023-26469	0.951470000	0.993750000	Link
CVE-2023-26360	0.964390000	0.996150000	Link
CVE-2023-26035	0.969020000	0.997470000	Link
CVE-2023-25717	0.954250000	0.994260000	Link
CVE-2023-25194	0.966980000	0.996930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996040000	Link
CVE-2023-24489	0.973820000	0.999310000	Link
CVE-2023-23752	0.956380000	0.994640000	Link
CVE-2023-23333	0.961070000	0.995420000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.965200000	0.996390000	Link
CVE-2023-22515	0.972760000	0.998880000	Link
CVE-2023-21839	0.955020000	0.994400000	Link
CVE-2023-21554	0.955880000	0.994570000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962690000	0.995720000	Link
CVE-2023-0669	0.971330000	0.998370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 03 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen oder um Daten zu manipulieren.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere

Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, Daten zu manipulieren, vertrauliche Informationen offenzulegen, eine Man-in-the-Middle-Situation zu schaffen, Sicherheitsmaßnahmen zu umgehen oder eine Denial-of-Service-Situation zu schaffen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 03 Sep 2024

[NEU] [hoch] VMware Fusion: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 03 Sep 2024

[NEU] [hoch] Zyxel Firewall: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in der Zyxel Firewall ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen oder Cross-Stie Scripting-Angriffe durchzuführen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Oracle Virtualization: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Secure Global Desktop und Oracle VM Virtual Box ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Intel Prozessoren: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Intel Prozessoren ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in QEMU ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU und libvirt: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU und libvirt ausnutzen, um Informationen offenzulegen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Tue, 03 Sep 2024

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

Ein lokaler Angreifer kann eine Schwachstelle in libvirt ausnutzen, um einen Denial of Service Zustand herbeizuführen oder um seine Privilegien zu erhöhen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstelle in QEMU ausnutzen, um einen Denial of Service Angriff durchzuführen und vertrauliche Informationen offenzulegen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Red Enterprise Linux Advanced Virtualization: Mehrere Schwachstellen

Ein entfernter oder lokaler, authentisierter Angreifer kann mehrere Schwachstellen in Red Enterprise Linux Advanced Virtualization ausnutzen, um einen Denial of Service zu verursachen, Sicherheitsvorkehrungen zu umgehen, beliebigen Code auszuführen und Informationen offenzulegen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um seine Privilegien zu erhöhen und vertrauliche Informationen offenzulegen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service zu verursachen.

- Link

—

Tue, 03 Sep 2024

[UPDATE] [hoch] QEMU: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstelle in QEMU ausnutzen, um einen Denial of Service Angriff durchzuführen und beliebigen Code auszuführen.

- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/3/2024	[Mozilla Firefox < 130.0]	critical
9/3/2024	[Mozilla Firefox < 130.0]	critical
9/3/2024	[Mozilla Firefox ESR < 115.15]	critical
9/3/2024	[Mozilla Firefox ESR < 115.15]	critical
9/3/2024	[Mozilla Firefox ESR < 128.2]	critical
9/3/2024	[Mozilla Firefox ESR < 128.2]	critical
9/3/2024	[Debian dla-3857 : libtommath-dev - security update]	critical
9/3/2024	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2024-247-01)]	critical
9/3/2024	[RHEL 8 : libproxy (RHSA-2024:6205)]	critical
9/3/2024	[RHEL 8 : emacs (RHSA-2024:6203)]	critical
9/3/2024	[RHEL 9 : krb5 (RHSA-2024:6166)]	critical
9/3/2024	[RHEL 9 : wget (RHSA-2024:6192)]	critical
9/3/2024	[Oracle Linux 9 : krb5 (ELSA-2024-6166)]	critical
9/3/2024	[Oracle Linux 9 : wget (ELSA-2024-6192)]	critical
9/3/2024	[FreeBSD : OpenSSL – Multiple vulnerabilities (21f505f4-6a1c-11ef-b611-84a93843eb75)]	critical
9/3/2024	[VMware Fusion 13.0.x < 13.6 Vulnerability (VMSA-2024-0018)]	high
9/3/2024	[Ubuntu 14.04 LTS : Drupal vulnerabilities (USN-6981-2)]	high
9/3/2024	[Ubuntu 22.04 LTS / 24.04 LTS : OpenSSL vulnerability (USN-6986-1)]	high

Datum	Schwachstelle	Bewertung
9/3/2024	[Debian dsa-5764 : libcrypto3-udeb - security update]	high
9/3/2024	[Slackware Linux 15.0 / current seamonkey Vulnerability (SSA:2024-247-02)]	high
9/3/2024	[RHEL 9 : kpatch-patch-5_14_0-427_13_1 and kpatch-patch-5_14_0-427_31_1 (RHSA-2024:6242)]	high
9/3/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Django vulnerabilities (USN-6987-1)]	high
9/3/2024	[FreeBSD : chromium – multiple security fixes (26125e09-69ca-11ef-8a0f-a8a1599412c6)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 03 Sep 2024

Texas Instruments Fusion Digital Power Designer 7.10.1 Credential Disclosure

Texas Instruments Fusion Digital Power Designer version 7.10.1 allows a local attacker to obtain sensitive information via the plaintext storage of credentials.

- Link

—

” “Tue, 03 Sep 2024

Taskhub 2.8.8 Insecure Settings

Taskhub version 2.8.8 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Webpay E-Commerce 1.0 SQL Injection

Webpay E-Commerce version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 03 Sep 2024

SPIP 4.2.9 Code Execution

SPIP version 4.2.9 suffers from a code execution vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Online Traffic Offense 1.0 Cross Site Request Forgery

Online Traffic Offense version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Penglead 2.0 Cross Site Scripting

Penglead version 2.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 03 Sep 2024

PPDB 2.4-update 6118-1 Cross Site Request Forgery

PPDB version 2.4-update 6118-1 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 03 Sep 2024

Online Travel Agency System 1.0 Arbitrary File Upload

Online Travel Agency System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Packet Storm New Exploits For August, 2024

This archive contains all of the 722 exploits added to Packet Storm in August, 2024. Please note the increase in size for this month is due to a massive backlog of older exploits being added to the archive and is not representative of an uptick in new issues being discovered.

- Link

—

” “Mon, 02 Sep 2024

IntelliNet 2.0 Remote Root

Zero day remote root exploit for IntelliNet version 2.0. It affects multiple devices of AES Corp and Siemens. The exploit provides a remote shell and escalates your permissions to full root permissions by abusing exec_suid. No authentication needed at all, neither any interaction from the victim. The firmware affected by this exploit runs on fire alarms, burglar sensors and environmental devices, all on the internet, all vulnerable, no patch. Full control over hardware and software with no restrictions, you can manipulate battery voltage and even damage the hardware with unknown outcomes.

- Link

—

” “Mon, 02 Sep 2024

Online Musical Instrument Shop IN 1.0 Cross Site Scripting

Online Musical Instrument Shop IN version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Online Job Portal IN 1.0 SQL Injection

Online Job Portal IN version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 02 Sep 2024

pgAdmin 8.4 Code Execution

pgAdmin versions 8.4 and earlier are affected by a remote reverse connection execution vulnerability via the binary path validation API.

- Link

—

” “Mon, 02 Sep 2024

SPIP 4.2.7 Code Execution

SPIP version 4.2.7 suffers from a code execution vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Loan Management System 2024 1.0 Insecure Settings

Loan Management System 2024 version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Hostel Management System 1.0 Arbitrary File Upload

Hostel Management System version 1.0 version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 02 Sep 2024

File Management System 1.0 Cross Site Request Forgery

File Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Faculty Evaluation System 1.0 Cross Site Request Forgery

Faculty Evaluation System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 02 Sep 2024

eClass LMS 6.2.0 Shell Upload

eClass LMS version 6.2.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 02 Sep 2024

Free Hospital Management System For Small Practices 1.0 CSRF

Free Hospital Management System for Small Practices version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Sun, 01 Sep 2024

Cerberus FTP Server SFTP Username Enumeration

This Metasploit module uses a dictionary to brute force valid usernames from Cerberus FTP server via SFTP. This issue affects all versions of the software older than 6.0.9.0 or 7.0.0.2 and is caused by a discrepancy in the way the SSH service handles failed logins for valid and invalid users. This issue was discovered by Steve Embling.

- Link

—

” “Sun, 01 Sep 2024

Libssh Authentication Bypass Scanner

This Metasploit module exploits an authentication bypass in libssh server code where a USERAUTH_SUCCESS message is sent in place of the expected USERAUTH_REQUEST message. libssh versions 0.6.0 through 0.7.5 and 0.8.0 through 0.8.3 are vulnerable. Note that this modules success depends on whether the server code can trigger the correct (shell/exec) callbacks despite only the state machines authenticated state being set. Therefore, you may or may not get a shell if the server requires additional code paths to be followed.

- Link

—

” “Sun, 01 Sep 2024

Juniper SSH Backdoor Scanner

This Metasploit module scans for the Juniper SSH backdoor (also valid on Telnet). Any username is required, and the password is «< %s(un=%s) = %u.

- Link

—

” “Sun, 01 Sep 2024

Apache Karaf Default Credentials Command Execution

This Metasploit module exploits a default misconfiguration flaw on Apache Karaf versions 2.x-4.x. The karaf user has a known default password, which can be used to login to the SSH service, and execute operating system commands from remote.

- Link

—

” “Sun, 01 Sep 2024

Eaton Xpert Meter SSH Private Key Exposure Scanner

Eaton Power Xpert Meters running firmware below version 12.x.x.x or below version 13.3.x.x ship with a public/private key pair that facilitate remote administrative access to the devices. Tested on: Firmware 12.1.9.1 and 13.3.2.10.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Private video

Vorschaubild Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-03	[gardenhomesmanagement.com]	ransomhub	Link
2024-09-03	[simson-maxwell.com]	cactus	Link
2024-09-03	[balboabayresort.com]	cactus	Link
2024-09-03	[flodraulic.com]	cactus	Link
2024-09-03	[mcphillips.co.uk]	cactus	Link
2024-09-03	[rangeramerican.com]	cactus	Link
2024-09-03	[Turman]	qilin	Link
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[www.amberbev.com]	ransomhub	Link
2024-09-02	[www.sanyo-bussan.co.jp]	ransomhub	Link
2024-09-02	[www.pokerspa.it]	ransomhub	Link
2024-09-02	[Removal.AI]	ransomhub	Link
2024-09-02	[Project Hospitality]	rhysida	Link
2024-09-02	[Shomof Group]	medusa	Link
2024-09-02	[www.sanyo-av.com]	ransomhub	Link
2024-09-02	[www.schneider.ch]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-01	[Quálitas México]	hunters	Link
2024-09-01	[welland]	trinity	Link

8 Quellen

8.1 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

9 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.