Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240903

Inhaltsverzeichnis

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

“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
—
Wordpress: 1 Million Webseiten nutzen verwundbares Plug-in WPML
Das Wordpress-Plug-in WPML kommt auf mehr als eine Million aktive Installationen. Jetzt wurde eine kritische Lücke darin gestopft.
- Link
—
Webbrowser: Weitere Lücke aktiv ausgenutzt, Adobe PDF-Viewer aktualisiert
Google meldet das Ausnutzen einer weiteren Lücke in freier Wildbahn. Die Updates von Edge schließen auch ein Leck im Adobe PDF Viewer.
- 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	0.991690000	Link
CVE-2023-6895	0.921160000	0.990120000	Link
CVE-2023-6553	0.921020000	0.990100000	Link
CVE-2023-6019	0.918710000	0.989870000	Link
CVE-2023-5360	0.902780000	0.988850000	Link
CVE-2023-52251	0.946410000	0.992930000	Link
CVE-2023-4966	0.970940000	0.998190000	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	0.993550000	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	0.995550000	Link
CVE-2023-42793	0.971190000	0.998300000	Link
CVE-2023-41265	0.911110000	0.989390000	Link
CVE-2023-39143	0.940480000	0.992150000	Link
CVE-2023-38646	0.906950000	0.989110000	Link
CVE-2023-38205	0.953670000	0.994160000	Link
CVE-2023-38203	0.965830000	0.996590000	Link
CVE-2023-38146	0.920720000	0.990060000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-38035	0.974690000	0.999730000	Link
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	0.997970000	Link
CVE-2023-34993	0.973540000	0.999190000	Link
CVE-2023-34960	0.921610000	0.990190000	Link
CVE-2023-34634	0.923140000	0.990330000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.952470000	0.993960000	Link
CVE-2023-3368	0.942130000	0.992340000	Link
CVE-2023-33246	0.967180000	0.996970000	Link
CVE-2023-32315	0.970220000	0.997880000	Link
CVE-2023-30625	0.953610000	0.994150000	Link
CVE-2023-30013	0.965950000	0.996620000	Link
CVE-2023-29300	0.969240000	0.997560000	Link
CVE-2023-29298	0.941540000	0.992290000	Link
CVE-2023-28432	0.907350000	0.989150000	Link
CVE-2023-28343	0.933130000	0.991430000	Link
CVE-2023-28121	0.919520000	0.989950000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.973470000	0.999170000	Link
CVE-2023-27350	0.969720000	0.997720000	Link
CVE-2023-26469	0.951470000	0.993740000	Link
CVE-2023-26360	0.964390000	0.996140000	Link
CVE-2023-26035	0.969020000	0.997470000	Link
CVE-2023-25717	0.954250000	0.994250000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.966980000	0.996930000	Link
CVE-2023-2479	0.963960000	0.996030000	Link
CVE-2023-24489	0.973820000	0.999310000	Link
CVE-2023-23752	0.956380000	0.994640000	Link
CVE-2023-23333	0.961070000	0.995410000	Link
CVE-2023-22527	0.968780000	0.997410000	Link
CVE-2023-22518	0.965200000	0.996390000	Link
CVE-2023-22515	0.972340000	0.998670000	Link
CVE-2023-21839	0.955020000	0.994400000	Link
CVE-2023-21554	0.955880000	0.994560000	Link
CVE-2023-20887	0.970840000	0.998140000	Link
CVE-2023-1671	0.962690000	0.995710000	Link
CVE-2023-0669	0.971330000	0.998370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 02 Sep 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Mon, 02 Sep 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Mon, 02 Sep 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libpng ausnutzen, um einen Denial of Service Angriff durchzuführen oder andere Angriffe mit nicht näher spezifizieren Auswirkungen zu starten.

- Link

—

Mon, 02 Sep 2024

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

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

- Link

—

Mon, 02 Sep 2024

[UPDATE] [hoch] cURL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um einen Denial of Service zu verursachen, Informationen offenzulegen oder weitere, nicht näher spezifizierte Angriffe durchzuführen.

- Link

—

Mon, 02 Sep 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 02 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 02 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 02 Sep 2024

[UPDATE] [UNGEPATCHT] [hoch] D-LINK Router DIR-846W: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen im D-LINK Router DIR-846W ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 30 Aug 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, UI-Spoofing zu betreiben, Sicherheitsmechanismen zu umgehen und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Fri, 30 Aug 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 30 Aug 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

Fri, 30 Aug 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

—

Fri, 30 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um

Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.
- Link

—

Fri, 30 Aug 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.
- Link

—

Fri, 30 Aug 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 30 Aug 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

—

Fri, 30 Aug 2024

[NEU] [hoch] Rockwell Automation FactoryTalk: Schwachstelle ermöglicht Privilegieneskalation und Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in Rockwell Automation FactoryTalk ausnutzen, um seine Privilegien zu erhöhen oder um beliebigen Code auszuführen.
- Link

—

Thu, 29 Aug 2024

[UPDATE] [hoch] Moodle: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Code auszuführen, bestimmte administrative Aufgaben durchzuführen, Informationen preiszugeben, Daten zu manipulieren, Sicherheitsmechanismen zu umgehen, Cross-Site-Scripting-Angriffe durchzuführen und eine nicht näher spezifizierte Wirkung zu erzielen.

- Link

—

Thu, 29 Aug 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Angriff durchführen, beliebigen Programmcode ausführen oder sensible Informationen ausspähen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/2/2024	[Emerson Ovation Missing Authentication for Critical Function (CVE-2022-29966)]	critical
9/2/2024	[Emerson Ovation Insufficient Verification of Data Authenticity (CVE-2022-30267)]	critical
8/31/2024	[Fedora 40 : python3.11 (2024-985017d277)]	critical
8/30/2024	[Apache OFBiz < 18.12.15 Remote Code Execution (CVE-2024-38856)]	critical
8/30/2024	[Debian dsa-5763 : python-pymatgen-doc - security update]	critical
9/2/2024	[Fedora 39 : microcode_ctl (2024-dca1b54441)]	high
9/2/2024	[Ubuntu 24.04 LTS : Dovecot vulnerabilities (USN-6982-1)]	high
9/2/2024	[Debian dla-3860 : dovecot-auth-lua - security update]	high
9/2/2024	[Debian dla-3858 : libruby2.7 - security update]	high
9/2/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : FFmpeg vulnerability (USN-6983-1)]	high
9/2/2024	[Debian dla-3862 : calibre - security update]	high
9/2/2024	[Oracle Linux 8 : virt:kvm_utils3 (ELSA-2024-12604)]	high

Datum	Schwachstelle	Bewertung
9/2/2024	[Oracle Linux 8 : virt:kvm_utils2 (ELSA-2024-12605)]	high
9/2/2024	[Ubuntu 18.04 LTS : Linux kernel (Raspberry Pi) vulnerabilities (USN-6973-4)]	high
9/2/2024	[Rockwell GuardLogix/ControlLogix 5580 Controller denial-of-service Vulnerability via Malformed Packet Handling (CVE-2024-40619)]	high
9/2/2024	[Rockwell Automation ControlLogix, GuardLogix, and CompactLogix Improper Input Validation (CVE-2024-7507)]	high
9/2/2024	[Rockwell ControlLogix, GuardLogix 5580, CompactLogix, and Compact GuardLogix 5380 Improper Input Validation (CVE-2024-7515)]	high
8/31/2024	[Fedora 39 : xen (2024-ed546e3543)]	high
8/31/2024	[Fedora 40 : xen (2024-91ddad6c8b)]	high
8/31/2024	[SUSE SLES12 Security Update : apache2 (SUSE-SU-2024:3061-1)]	high
8/31/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0267-1)]	high
8/31/2024	[Fedora 40 : microcode_ctl (2024-5c5c384fa7)]	high
8/31/2024	[FreeBSD : forgejo – The scope of application tokens was not verified when writing containers or Conan packages. (eb437e17-66a1-11ef-ac08-75165d18d8d2)]	high
8/30/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-26934)]	high
8/30/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-27020)]	high
8/30/2024	[CBL Mariner 2.0 Security Update: python-pygments (CVE-2021-27291)]	high
8/30/2024	[Oracle Linux 8 : postgresql:13 (ELSA-2024-6018)]	high
8/30/2024	[Oracle Linux 8 : postgresql:15 (ELSA-2024-6001)]	high
8/30/2024	[Oracle Linux 8 : postgresql:12 (ELSA-2024-6000)]	high
8/30/2024	[Oracle Linux 9 : postgresql:15 (ELSA-2024-6020)]	high

Datum	Schwachstelle	Bewertung
8/30/2024	[FreeBSD : firefox – multiple vulnerabilities (5e4d7172-66b8-11ef-b104-b42e991fc52e)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Sun, 01 Sep 2024

SSH Username Enumeration

This Metasploit module uses a malformed packet or timing attack to enumerate users on an OpenSSH server. The default action sends a malformed (corrupted) SSH_MSG_USERAUTH_REQUEST packet using public key authentication (must be enabled) to enumerate users. On some versions of OpenSSH under some configurations, OpenSSH will return a ”permission denied” error for an invalid user faster than for a valid user, creating an opportunity for a timing attack to enumerate users. Testing note: invalid users were logged, while valid users were not. YMMV.

- Link

—

” “Sun, 01 Sep 2024

Fortinet SSH Backdoor Scanner

This Metasploit module scans for the Fortinet SSH backdoor.

- Link

—

” “Sun, 01 Sep 2024

MySQL Authentication Bypass Password Dump

This Metasploit module exploits a password bypass vulnerability in MySQL in order to extract the usernames and encrypted password hashes from a MySQL server. These hashes are stored as loot for later cracking. Impacts MySQL versions: - 5.1.x before 5.1.63 - 5.5.x before 5.5.24 - 5.6.x before 5.6.6 And MariaDB versions: - 5.1.x before 5.1.62 - 5.2.x before 5.2.12 - 5.3.x before 5.3.6 - 5.5.x before 5.5.23.

- Link

—

” “Sun, 01 Sep 2024

DNS Amplification Scanner

This Metasploit module can be used to discover DNS servers which expose recursive name lookups which can be used in an amplification attack against a third party.

- Link

—

” “Sun, 01 Sep 2024

Novell ZENworks Configuration Management Preboot Service Remote File Access

This Metasploit module exploits a directory traversal in the ZENworks Configuration Management. The vulnerability exists in the Preboot service and can be triggered by sending a specially crafted PROXY_CMD_FTP_FILE (opcode 0x21) packet to the 998/TCP port. This Metasploit module has been

successfully tested on Novell ZENworks Configuration Management 10 SP2 and SP3 over Windows.
- Link

—

” “Sun, 01 Sep 2024

Ray Sharp DVR Password Retriever

This Metasploit module takes advantage of a protocol design issue with the Ray Sharp based DVR systems. It is possible to retrieve the username and password through the TCP service running on port 9000. Other brands using this platform and exposing the same issue may include Swann, Lorex, Night Owl, Zmodo, URMET, and KGuard Security.
- Link

—

” “Sun, 01 Sep 2024

Dahua DVR Authentication Bypass Scanner

This Metasploit modules scans for Dahua-based DVRs and then grabs settings. Optionally resets a users password and clears the device logs.
- Link

—

” “Sun, 01 Sep 2024

Rosewill RXS-3211 IP Camera Password Retriever

This Metasploit module takes advantage of a protocol design issue with the Rosewill admin executable in order to retrieve passwords, allowing remote attackers to take administrative control over the device. Other similar IP Cameras such as Edimax, Hawking, Zonet, etc, are also believed to have the same flaw, but not fully tested. The protocol design issue also allows attackers to reset passwords on the device.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 30 Aug 2024

ZDI-24-1192: (0Day) Visteon Infotainment REFLASH_DDU_ExtractFile Command Injection Remote Code Execution Vulnerability
- Link

—

” “Fri, 30 Aug 2024

ZDI-24-1191: (0Day) Visteon Infotainment REFLASH_DDU_FindFile Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 30 Aug 2024

ZDI-24-1190: (0Day) Visteon Infotainment UPDATES_ExtractFile Command Injection Remote Code Execution Vulnerability

- Link

—

” “Fri, 30 Aug 2024

ZDI-24-1189: (0Day) Visteon Infotainment App SoC Missing Immutable Root of Trust in Hardware Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 30 Aug 2024

ZDI-24-1188: (0Day) Visteon Infotainment VIP MCU Code Insufficient Validation of Data Authenticity Local Privilege Escalation Vulnerability

- Link

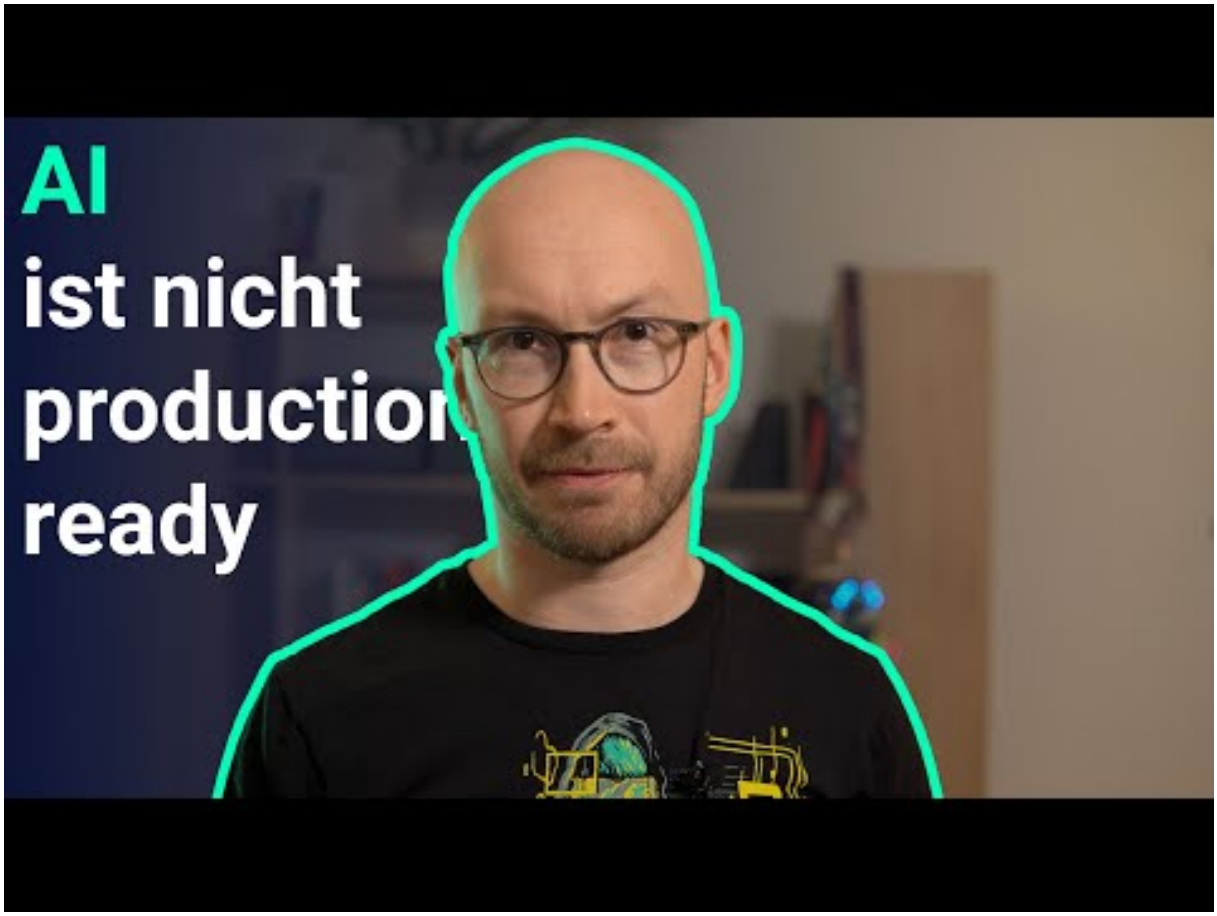
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AI ist nicht bereit für Production (Indirekte Prompt Injection in der Slack AI)



Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.