Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241002

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

Web-Config von Seiko-Epson-Geräten ermöglicht Angreifern Übernahme

Das Web-Interface von Geräten wie Druckern von Seiko-Epson ermöglicht Angreifern in vielen Fällen, diese als Administrator zu übernehmen.

- Link

—

CERT-Bund warnt: Mehr als 15.000 Exchange-Server mit Sicherheitslücken

In Deutschland stehen noch immer mehr als 15.000 Exchange-Server mit mindestens einer Codeschmuggel-Lücke offen im Netz, warnt das CERT-Bund.

- Link

—

Monitoring-Software Whatsup Gold: Hersteller rät zum schleunigen Update

Progress warnt, dass teils kritische Sicherheitslücken in Whatsup Gold lauern. Admins sollen so schnell wie möglich aktualisieren.

- Link

—

Kritische Sicherheitslücken: PHP 8.3.12, 8.2.24 und 8.1.30 dichten Lecks ab

Die PHP-Entwickler haben PHP 8.3.12, 8.2.24 und 8.1.30 veröffentlicht. Darin schließen sie mehrere, teils kritische Sicherheitslücken.

- Link

—

Foxit PDF: Manipulierte PDFs können Schadcode durchschleusen

Es sind gegen verschiedene Attacken gerüstete Versionen von Foxit PDF Editor und PDF Reader für macOS und Windows erschienen.

- Link

—

Teils kritische Lücken in Unix-Drucksystem CUPS ermöglichen Codeschmuggel

Im Linux-Drucksystem CUPS wurden teils kritische Sicherheitslücken entdeckt. Angreifer können dadurch etwa Code einschmuggeln.

- Link

—

Schadcode-Schlupfloch in Nvidia Container Toolkit geschlossen

Angreifer können an Sicherheitslücken in Nvidia Container Toolkit und GPU Operator ansetzen, um Systeme zu kompromittieren.

- Link

—

Sicherheitsupdates: DoS-Angriffe auf Cisco-Netzwerkhardware möglich

Aufgrund von mehreren Sicherheitslücken in Ciscos Netzwerkbetriebssystem IOS XE sind verschiedene Geräte verwundbar. Patches stehen zum Download.

- Link

—

Progress Telerik: hochriskante Lücken erlauben Code- und Befehlsschmuggel

In Progress Telerik UI for WPF und WinForms können Angreifer aufgrund von Sicherheitslücken Schadcode und Befehle einschmuggeln.

- Link

—

Teamviewer: Hochriskante Lücken ermöglichen Rechteausweitung

In der Fernwartungssoftware Teamviewer klaffen Sicherheitslücken, durch die Angreifer ihre Rechte ausweiten können. Updates schließen sie.

- 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	0.957580000	0.994820000	Link
CVE-2023-6895	0.927330000	0.990790000	Link
CVE-2023-6553	0.947820000	0.993180000	Link
CVE-2023-6019	0.918710000	0.989940000	Link
CVE-2023-52251	0.949200000	0.993380000	Link
CVE-2023-4966	0.970840000	0.998160000	Link
CVE-2023-49103	0.949680000	0.993480000	Link
CVE-2023-48795	0.964670000	0.996200000	Link
CVE-2023-47246	0.960360000	0.995250000	Link
CVE-2023-46805	0.957170000	0.994760000	Link
CVE-2023-46747	0.971540000	0.998420000	Link
CVE-2023-46604	0.970850000	0.998170000	Link
CVE-2023-4542	0.944110000	0.992630000	Link
CVE-2023-43208	0.974060000	0.999420000	Link
CVE-2023-43177	0.958390000	0.994940000	Link
CVE-2023-42793	0.970970000	0.998220000	Link
CVE-2023-41265	0.907590000	0.989190000	Link
CVE-2023-39143	0.940700000	0.992220000	Link
CVE-2023-38205	0.949280000	0.993390000	Link
CVE-2023-38203	0.964750000	0.996250000	Link
CVE-2023-38146	0.919150000	0.989990000	Link
CVE-2023-38035	0.974550000	0.999660000	Link
CVE-2023-36845	0.967920000	0.997180000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996590000	Link
CVE-2023-35082	0.967900000	0.997170000	Link
CVE-2023-35078	0.971130000	0.998290000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34960	0.900520000	0.988760000	Link
CVE-2023-34634	0.923140000	0.990370000	Link
CVE-2023-34362	0.970450000	0.998010000	Link
CVE-2023-34105	0.927500000	0.990810000	Link
CVE-2023-34039	0.943770000	0.992580000	Link
CVE-2023-3368	0.942240000	0.992380000	Link
CVE-2023-33246	0.969870000	0.997810000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953820000	0.994210000	Link
CVE-2023-30013	0.965950000	0.996600000	Link
CVE-2023-29300	0.967820000	0.997120000	Link
CVE-2023-29298	0.969390000	0.997610000	Link
CVE-2023-28432	0.921930000	0.990270000	Link
CVE-2023-28343	0.937460000	0.991850000	Link
CVE-2023-28121	0.922260000	0.990300000	Link
CVE-2023-27524	0.970600000	0.998060000	Link
CVE-2023-27372	0.974150000	0.999480000	Link
CVE-2023-27350	0.968980000	0.997480000	Link
CVE-2023-26469	0.953540000	0.994150000	Link
CVE-2023-26360	0.964630000	0.996190000	Link
CVE-2023-26035	0.968720000	0.997400000	Link
CVE-2023-25717	0.950620000	0.993610000	Link
CVE-2023-25194	0.964550000	0.996160000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995840000	Link
CVE-2023-24489	0.972860000	0.998910000	Link
CVE-2023-23752	0.952050000	0.993870000	Link
CVE-2023-23333	0.960430000	0.995270000	Link
CVE-2023-22527	0.970500000	0.998030000	Link
CVE-2023-22518	0.959950000	0.995210000	Link
CVE-2023-22515	0.973910000	0.999360000	Link
CVE-2023-21839	0.947720000	0.993160000	Link
CVE-2023-21554	0.952650000	0.994000000	Link
CVE-2023-20887	0.970950000	0.998220000	Link
CVE-2023-1698	0.917150000	0.989810000	Link
CVE-2023-1671	0.962220000	0.995620000	Link
CVE-2023-0669	0.971830000	0.998500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 01 Oct 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 01 Oct 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, 01 Oct 2024

[NEU] [hoch] Octopus Deploy: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Octopus Deploy ausnutzen, um Informationen offenzulegen.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Net-SNMP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Net-SNMP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Tue, 01 Oct 2024

[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

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Erlangung erweiterter Privilegien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um erweiterte Privilegien zu erlangen.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 01 Oct 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Tue, 01 Oct 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

—

Tue, 01 Oct 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in AMD Prozessor und AMD Radeon ausnutzen, um beliebigen Programmcode auszuführen, erhöhte Rechte zu erlangen, einen Denial-of-Service-Zustand zu erzeugen, Daten zu manipulieren, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen preiszugeben.

- Link

—

Tue, 01 Oct 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder Daten zu manipulieren.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Tue, 01 Oct 2024

[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- Link

—

Mon, 30 Sep 2024

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

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

- Link

—

Mon, 30 Sep 2024

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

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

- Link

—

Mon, 30 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

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Codeausführung

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/1/2024	[Synology DiskStation Manager Netatalk Out-of-bounds Write (CVE-2018-1160)]	critical
10/1/2024	[Synology DiskStation Manager SQL Injection (CVE-2021-43927)]	critical
10/1/2024	[Synology DiskStation Manager Permissions, Privileges, and Access Controls (CVE-2013-6955)]	critical
10/1/2024	[Synology DiskStation Manager Exposure of Sensitive Information to an Unauthorized Actor (CVE-2018-8919)]	critical
10/1/2024	[Synology DiskStation Manager Exposure of Sensitive Information to an Unauthorized Actor (CVE-2021-26566)]	critical
10/1/2024	[Synology DiskStation Manager Dnsmasq Out-of-bounds Write (CVE-2017-14491)]	critical
10/1/2024	[Synology DiskStation Manager Use After Free (CVE-2021-27646)]	critical
10/1/2024	[Synology DiskStation Manager Improper Certificate Validation (CVE-2020-27648)]	critical
10/1/2024	[Synology DiskStation Manager Use After Free (CVE-2021-27649)]	critical
10/1/2024	[Synology DiskStation Manager OS Command Injection (CVE-2018-13284)]	high
10/1/2024	[Synology DiskStation Manager Uncontrolled Search Path Element (CVE-2023-0142)]	high
10/1/2024	[Synology DiskStation Manager Path Traversal (CVE-2021-29088)]	high

Datum	Schwachstelle	Bewertung
10/1/2024	[Synology DSM HTTP/2 Implementations Allocation of Resources Without Limits or Throttling (CVE-2019-9517)]	high
10/1/2024	[Synology DiskStation Manager SYNO.API.Encryption API Protection Mechanism Bypass (CVE-2017-9553)]	high
10/1/2024	[Synology DiskStation Manager Exposure of Sensitive Information to an Unauthorized Actor (CVE-2022-22680)]	high
10/1/2024	[Synology DiskStation Manager NTPD Denial of Service (CVE-2018-7184)]	high
10/1/2024	[Synology DiskStation Manager Exposure of Sensitive Information to an Unauthorized Actor (CVE-2021-29086)]	high
10/1/2024	[Synology DiskStation Manager Path Traversal (CVE-2022-27610)]	high
10/1/2024	[Synology DiskStation Manager Exposure of Sensitive Information to an Unauthorized Actor (CVE-2014-2264)]	high
10/1/2024	[Synology DiskStation Manager Race Condition (CVE-2022-27626)]	high
10/1/2024	[Synology DiskStation Manager Race Condition (CVE-2021-26569)]	high
10/1/2024	[Synology DiskStation Manager Command Injection (CVE-2017-15889)]	high
10/1/2024	[Synology DSM HTTP/2 Implementations Uncontrolled Resource Consumption (CVE-2019-9513)]	high
10/1/2024	[Synology DiskStation Manager Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-26561)]	high
10/1/2024	[Synology DiskStation Manager Improper Encoding or Escaping of Output (CVE-2018-8920)]	high
10/1/2024	[Synology DiskStation Manager Injection (CVE-2021-29085)]	high
10/1/2024	[Synology DiskStation Manager Samba Out-of-bounds Read (CVE-2021-44142)]	high

Datum	Schwachstelle	Bewertung
10/1/2024	[Synology DiskStation FAAD2 Decoder Out-of-bounds Write (CVE-2021-26567)]	high
10/1/2024	[Synology DiskStation Manager Out-of-bounds Write (CVE-2021-26562)]	high
10/1/2024	[Synology DSM HTTP/2 Implementations Window Size and Stream Prioritization Manipulation (CVE-2019-9511)]	high
10/1/2024	[Synology DiskStation Manager OS Command Injection (CVE-2021-29083)]	high
10/1/2024	[Synology DiskStation Manager Path Traversal (CVE-2013-6987)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 01 Oct 2024

Packet Storm New Exploits For September, 2024

This archive contains all of the 522 exploits added to Packet Storm in September, 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

—

” “Tue, 01 Oct 2024

Nitro PDF Pro Local Privilege Escalation

The Nitro PDF Pro application uses a .msi installer file (embedded into an executable .exe installer file) for installation. The MSI installer uses custom actions in repair mode in an unsafe way. Attackers with low-privileged system access to a Windows system where Nitro PDF Pro is installed, can exploit the cached MSI installer’s custom actions to effectively escalate privileges and get a command prompt running in context of NT AUTHORITY\SYSTEM. Versions prior to 14.26.1.0 and 13.70.8.82 and affected.

- Link

—

” “Tue, 01 Oct 2024

VICIdial Authenticated Remote Code Execution

An attacker with authenticated access to VICIdial as an ”agent” can execute arbitrary shell commands as the ”root” user. This attack can be chained with CVE-2024-8503 to execute arbitrary shell commands starting from an unauthenticated perspective.

- Link

—

” “Tue, 01 Oct 2024

Student Study Center Management System 1.0 Insecure Settings

Student Study Center Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 01 Oct 2024

Student Management System 1.0 Insecure Settings

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

- Link

—

” “Tue, 01 Oct 2024

Student Attendance Management System 1.0 Code Injection

Student Attendance Management System version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Tue, 01 Oct 2024

Simple Music Management System 1.0 Arbitrary File Upload

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

- Link

—

” “Tue, 01 Oct 2024

Printing Business Records Management System 1.0 Arbitrary File Upload

Printing Business Records Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 01 Oct 2024

Online Tourism Management System 1.0 Insecure Settings

Online Tourism Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 01 Oct 2024

Online Eyewear Shop 1.0 Arbitrary File Upload

Online Eyewear Shop version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 01 Oct 2024

Event Management System 1.0 Arbitrary File Upload

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

- Link

—

” “Mon, 30 Sep 2024

VegaBird Vooki 5.2.9 DLL Hijacking

VegaBird Vooki version 5.2.9 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 30 Sep 2024

VegaBird Yaazhini 2.0.2 DLL Hijacking

VegaBird Yaazhini version 2.0.2 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 30 Sep 2024

BlackBerry CylanceOPTICS Uninstall Password Bypass

BlackBerry CylanceOPTICS versions prior to 3.3 MR2 and 3.2 MR5 suffer from an uninstall password bypass vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Student Management System 1.0 Insecure Cookie Handling

Student Management System version 1.0 suffers from an insecure cookie handling vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Student Enrollment 1.0 Arbitrary File Upload

Student Enrollment version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Sistem Penyewaan Baju atau Pakaian Berbasis Web 1.0 SQL Injection

Sistem Penyewaan Baju atau Pakaian Berbasis Web version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 30 Sep 2024

Simple Student Quarterly Result / Grade System 1.0 Insecure Settings

Simple Student Quarterly Result / Grade System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Simple Responsive Tourism Website 1.0 Cross Site Request Forgery

Simple Responsive Tourism Website version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Simple Music Management System 1.0 Add Administrator / Cross Site Request Forgery

Simple Music Management System version 1.0 suffers from add administrator and cross site request forgery vulnerabilities.

- Link

—

” “Mon, 30 Sep 2024

Sample Blog Site 1.0 Cross Site Scripting / Remote File Inclusion

Sample Blog Site version 1.0 suffers from cross site scripting and remote file inclusion vulnerabilities.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Benju.a MVID-2024-0700 Remote Command Execution

Backdoor.Win32.Benju.a malware suffers from a remote command execution vulnerability. This is the 700th release of a malvuln finding.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Prorat.jz MVID-2024-0699 Buffer Overflow

Backdoor.Win32.Prorat.jz malware suffers from a buffer overflow vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Amatu.a MVID-2024-0698 Arbitrary File Write

Backdoor.Win32.Amatu.a malware suffers from a remote arbitrary file write vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Agent.pw MVID-2024-0697 Buffer Overflow

Backdoor.Win32.Agent.pw malware suffers from a buffer overflow vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.

Zum Youtube Video

6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information

7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-10-01	[Acuity Advisor]	stormous	Link
2024-10-01	[United Animal Health]	qilin	Link
2024-10-01	[Akromold]	nitrogen	Link
2024-10-01	[Labib Funk Associates]	nitrogen	Link
2024-10-01	[Research Electronics International]	nitrogen	Link
2024-10-01	[Cascade Columbia Distribution]	akira	Link
2024-10-01	[ShoreMaster]	akira	Link
2024-10-01	[marthamedeiros.com.br]	madliberator	Link
2024-10-01	[CSG Consultants]	akira	Link
2024-10-01	[aberdeenwa.gov]	ElDorado	Link
2024-10-01	[Corantioquia]	meow	Link
2024-10-01	[performance-therapies]	qilin	Link
2024-10-01	[www.galab.com]	cactus	Link
2024-10-01	[telehealthcenter.in]	killsec	Link
2024-10-01	[howardcpas.com]	ElDorado	Link
2024-10-01	[bshsoft.com]	ElDorado	Link
2024-10-01	[credihealth.com]	killsec	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.