Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240914

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

Lenovo schließt Lücken in BIOS, Management-Controller und WLAN-Treiber
Wichtige Sicherheitsupdates schützen Computer von Lenovo. Im schlimmsten Fall können Angreifer Schadcode ausführen.
- Link

—

Solarwinds ARM: Unbefugte Zugriffe und Schadcode-Attacken möglich
Die Solarwinds-Entwickler haben zwei Sicherheitslücken in Access Rights Manager geschlossen. Eine Lücke gilt als kritisch.
- Link

—

Sicherheitspatch: Gitlab behebt Lücken in Serverversionen
Angreifer konnten Code einschleusen, fremde Konten übernehmen und den Server außer Gefecht setzen. Admins selbst gehosteter Instanzen sollten patchen.
- Link

—

Cisco: DoS- und Rechteausweitungslücken in IOS und weiteren Produkten
In Ciscos IOS und weiteren Produkten klaffen Sicherheitslücken. Angreifer können ihre Rechte ausweiten oder Geräte lahmlegen.
- Link

—

Ivanti: Updates gegen kritische Lecks im Endpoint Manager und weiteren Produkten
Ivanti bessert Schwachstellen in Endpoint Manager, Workspace Control und Cloud Service Appliance aus. Eine Lücke in EPM erreicht die Höchstwertung CVSS 10.
- Link

—

ownCloud: Update stopft teils hochriskante Sicherheitslücken
Das ownCloud-Projekt warnt vor Sicherheitslücken in der Kollaborationssoftware. Angreifer können etwa Zugriff auf Zugangsdaten erlangen.
- Link

—

Citrix Workspace App für Windows ermöglicht Rechteausweitung
In der Citrix Workspace App für Windows klaffen zwei Sicherheitslücken. Angreifer können dadurch ihre Rechte im System ausweiten.
- Link

—

Adobe-Patchday: Kritische Lücken in mehreren Produkten

Adobe stopft am Patchday mehrere kritische Sicherheitslecks. Updates gibt es für acht Produkte des Herstellers.

- Link

—

Patchday Microsoft: Angreifer attackieren vier Lücken in Windows & Co.

Microsoft hat Schwachstellen in unter anderem Azure, SharePoint und Windows geschlossen. Einige Lücken gelten als kritisch.

- Link

—

CISA warnt: Acht Jahre alte Lücke in ImageMagick und weitere angegriffen

Die CISA warnt, dass in ImageMagick eine acht Jahre alte Sicherheitslücke angegriffen wird. Ebenso eine sieben Jahre alte Lücke in Linux.

- 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	0.957050000	0.994790000	Link
CVE-2023-6895	0.921160000	0.990180000	Link
CVE-2023-6553	0.937150000	0.991840000	Link
CVE-2023-6019	0.918710000	0.989960000	Link
CVE-2023-5360	0.902780000	0.988910000	Link
CVE-2023-52251	0.945480000	0.992840000	Link
CVE-2023-4966	0.970840000	0.998140000	Link
CVE-2023-49103	0.949680000	0.993510000	Link
CVE-2023-48795	0.965330000	0.996480000	Link
CVE-2023-47246	0.956040000	0.994620000	Link
CVE-2023-46805	0.950230000	0.993610000	Link
CVE-2023-46747	0.972260000	0.998660000	Link
CVE-2023-46604	0.968800000	0.997430000	Link
CVE-2023-4542	0.948590000	0.993320000	Link
CVE-2023-43208	0.973970000	0.999390000	Link
CVE-2023-43177	0.961480000	0.995550000	Link
CVE-2023-42793	0.971190000	0.998310000	Link
CVE-2023-41265	0.907590000	0.989210000	Link
CVE-2023-39143	0.936490000	0.991780000	Link
CVE-2023-38205	0.950330000	0.993620000	Link
CVE-2023-38203	0.965830000	0.996630000	Link
CVE-2023-38146	0.920720000	0.990130000	Link
CVE-2023-38035	0.974690000	0.999730000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996880000	Link
CVE-2023-3519	0.965910000	0.996650000	Link
CVE-2023-35082	0.967460000	0.997070000	Link
CVE-2023-35078	0.970930000	0.998180000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34960	0.921610000	0.990250000	Link
CVE-2023-34634	0.923140000	0.990380000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.947070000	0.993070000	Link
CVE-2023-3368	0.939780000	0.992150000	Link
CVE-2023-33246	0.967830000	0.997170000	Link
CVE-2023-32315	0.971490000	0.998420000	Link
CVE-2023-30625	0.953610000	0.994200000	Link
CVE-2023-30013	0.965950000	0.996660000	Link
CVE-2023-29300	0.969240000	0.997570000	Link
CVE-2023-29298	0.970810000	0.998110000	Link
CVE-2023-28432	0.907350000	0.989190000	Link
CVE-2023-28343	0.933130000	0.991470000	Link
CVE-2023-28121	0.925430000	0.990620000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.973930000	0.999360000	Link
CVE-2023-27350	0.968480000	0.997340000	Link
CVE-2023-26469	0.953890000	0.994250000	Link
CVE-2023-26360	0.964390000	0.996170000	Link
CVE-2023-26035	0.968440000	0.997320000	Link
CVE-2023-25717	0.954660000	0.994380000	Link
CVE-2023-25194	0.966980000	0.996940000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996070000	Link
CVE-2023-24489	0.973820000	0.999320000	Link
CVE-2023-23752	0.951460000	0.993800000	Link
CVE-2023-23333	0.960430000	0.995320000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.961800000	0.995610000	Link
CVE-2023-22515	0.972760000	0.998900000	Link
CVE-2023-21839	0.951270000	0.993730000	Link
CVE-2023-21554	0.955880000	0.994590000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962690000	0.995770000	Link
CVE-2023-0669	0.971300000	0.998370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 13 Sep 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- Link

—

Fri, 13 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

—

Fri, 13 Sep 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, 13 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Fri, 13 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

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Apache OFBiz: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache OFBiz ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Adobe Acrobat Reader: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe Acrobat Reader, Adobe Acrobat, Adobe Acrobat Reader DC und Adobe Acrobat DC ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen ausnutzen oder nicht näher beschriebene Auswirkungen zu erzielen.

- Link

—

Fri, 13 Sep 2024

[NEU] [hoch] Kemp LoadMaster: Schwachstelle ermöglicht Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Kemp LoadMaster ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 13 Sep 2024

[NEU] [hoch] Mehrere NetApp Produkte: Schwachstelle ermöglicht Denial of Service, Offenlegung von Informationen und Manipulation von Daten

Ein anonymer Remote-Angreifer kann eine Schwachstelle in verschiedenen NetApp Produkten ausnutzen, um vertrauliche Informationen offenzulegen, Daten zu manipulieren oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 13 Sep 2024

[NEU] [hoch] Rockwell Automation FactoryTalk: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Rockwell Automation FactoryTalk ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- Link

—

Thu, 12 Sep 2024

[NEU] [hoch] GitLab CE/EE: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, beliebigen Code auszuführen, erhöhte Rechte zu erlangen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Thu, 12 Sep 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Thu, 12 Sep 2024

[NEU] [hoch] Cisco NSO und Router: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Cisco Network Services Orchestrator und Cisco Router ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Thu, 12 Sep 2024

[NEU] [hoch] Cisco IOS XR: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco IOS XR ausnutzen, um einen Denial of Service Angriff durchzuführen, erhöhte Rechte zu erlangen und vertrauliche Informationen preiszugeben.
- Link

—

Thu, 12 Sep 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

—

Thu, 12 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

—

Thu, 12 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

—

Thu, 12 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

—

Thu, 12 Sep 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
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : expat (SUSE-SU-2024:3216-1)]	critical
9/13/2024	[SUSE SLES15 / openSUSE 15 Security Update : containerd (SUSE-SU-2024:3221-1)]	critical
9/13/2024	[FreeBSD : Gitlab – vulnerabilities (bcc8b21e-7122-11ef-bece-2cf05da270f3)]	critical
9/13/2024	[Adobe ColdFusion < 2021.x < 2021u16 / 2023.x < 2023u10 Vulnerability (APSB24-71)]	critical
9/13/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-7007-1)]	critical
9/13/2024	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-7003-3)]	critical
9/13/2024	[Apache OFBiz < 18.12.16 Multiple Vulnerabilities]	critical
9/13/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-7009-1)]	critical
9/13/2024	[Ivanti Endpoint Manager 2024 - September 2024 Security Update]	critical
9/13/2024	[Debian dsa-5769 : git - security update]	critical
9/13/2024	[Oracle Linux 7 : httpd (ELSA-2024-4943)]	critical
9/12/2024	[Beckhoff (CVE-2024-41174)]	critical

Datum	Schwachstelle	Bewertung
9/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.23 (SUSE-SU-2024:3214-1)]	high
9/13/2024	[SUSE SLES15 Security Update : 389-ds (SUSE-SU-2024:3218-1)]	high
9/13/2024	[SUSE SLES15 Security Update : postgresql16 (SUSE-SU-2024:3158-2)]	high
9/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.22 (SUSE-SU-2024:3213-1)]	high
9/13/2024	[Fedora 40 : haproxy (2024-39913e097a)]	high
9/13/2024	[Photon OS 5.0: Linux PHSA-2024-5.0-0374]	high
9/13/2024	[SUSE SLES12 Security Update : postgresql16 (SUSE-SU-2024:3224-1)]	high
9/13/2024	[macOS 14.x < 14.6 Multiple Vulnerabilities (120911)]	high
9/13/2024	[macOS 13.x < 13.6.8 Multiple Vulnerabilities (120912)]	high
9/13/2024	[Security Updates for Azure CycleCloud (September 2024)]	high
9/13/2024	[Security Updates for Microsoft Office Online Server (September 2024)]	high
9/13/2024	[Cisco IOS XR Software UDP Packet Memory Exhaustion (cisco-sa-pak-mem-exhst-3ke9FeFy)]	high
9/13/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-7008-1)]	high
9/13/2024	[Citrix Workspace App for Windows Multiple Vulnerabilities (CTX691485)]	high
9/13/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-7005-2)]	high
9/13/2024	[RHEL 7 : python3-setuptools (RHSA-2024:6661)]	high
9/13/2024	[RHEL 7 : python-setuptools (RHSA-2024:6662)]	high
9/13/2024	[RHEL 8 : kpatch-patch-4_18_0-305_120_1 and kpatch-patch-4_18_0-305_138_1 (RHSA-2024:6663)]	high

Datum	Schwachstelle	Bewertung
9/13/2024	[Dell 2335dn printer Weak Password Requirements (CVE-2018-15748)]	high
9/12/2024	[Beckhoff (CVE-2024-41176)]	high
9/12/2024	[Beckhoff (CVE-2024-41173)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 13 Sep 2024

Ivanti EPM Remote Code Execution

Proof of concept remote code execution exploit for Ivanti EPM versions prior to 2022 SU6 or the 2024 September update.

- Link

—

” “Fri, 13 Sep 2024

GeoServer Remote Code Execution

Proof of concept remote code execution exploit for GeoServer versions prior 2.23.6, 2.24.4, and 2.25.2.

- Link

—

” “Fri, 13 Sep 2024

Webpay E-Commerce 1.0 Cross Site Scripting

Webpay E-Commerce version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Men Salon Management System 2.0 PHP Code Injection

Men Salon Management System version 2.0 suffers from a php code injection vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Emergency Ambulance Hiring Portal 1.0 Insecure Settings

Emergency Ambulance Hiring Portal version 1.0 suffers from an ignored default credential vulnerabi-

lity.

- Link

—

” “Fri, 13 Sep 2024

Car Washing Management System 1.0 Insecure Settings

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

- Link

—

” “Fri, 13 Sep 2024

Bus Pass Management System 1.0 Insecure Settings

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

- Link

—

” “Fri, 13 Sep 2024

BP Monitoring Management System 1.0 Insecure Settings

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

- Link

—

” “Fri, 13 Sep 2024

Beauty Parlour And Saloon Management System 1.1 Insecure Cookie Handling

Beauty Parlour and Saloon Management System version 1.1 suffers from an insecure cooking handling vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Auto/Taxi Stand Management System 1.0 PHP Code Injection

Auto/Taxi Stand Management System version 1.0 suffers from a php code injection vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Art Gallery Management System 1.0 Insecure Settings

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

- Link

—

” “Thu, 12 Sep 2024

MPlayer Lite r33064 Buffer Overflow

This Metasploit module exploits a stack-based buffer overflow vulnerability in MPlayer Lite r33064,

caused by improper bounds checking of an URL entry. By persuading the victim to open a specially-crafted .M3U file, specifically by drag-and-dropping it to the player, a remote attacker can execute arbitrary code on the system.

- Link

—

” “Thu, 12 Sep 2024

Windows Escalate UAC Execute RunAs

This Metasploit module will attempt to elevate execution level using the ShellExecute undocumented RunAs flag to bypass low UAC settings.

- Link

—

” “Thu, 12 Sep 2024

SPIP BigUp 4.3.1 / 4.2.15 / 4.1.17 Unauthenticated Remote Code Execution

This Metasploit module exploits a Remote Code Execution vulnerability in the BigUp plugin of SPIP. The vulnerability lies in the lister_fichiers_par_champs function, which is triggered when the bigup_retrouver_fichiers parameter is set to any value. By exploiting the improper handling of multipart form data in file uploads, an attacker can inject and execute arbitrary PHP code on the target server. This critical vulnerability affects all versions of SPIP from 4.0 up to and including 4.3.1, 4.2.15, and 4.1.17. It allows unauthenticated users to execute arbitrary code remotely via the public interface. The vulnerability has been patched in versions 4.3.2, 4.2.16, and 4.1.18.

- Link

—

” “Thu, 12 Sep 2024

QNX Qconn Command Execution

This Metasploit module uses the qconn daemon on QNX systems to gain a shell. The QNX qconn daemon does not require authentication and allows remote users to execute arbitrary operating system commands. This Metasploit module has been tested successfully on QNX Neutrino 6.5.0 (x86) and 6.5.0 SP1 (x86).

- Link

—

” “Thu, 12 Sep 2024

UnRAR Path Traversal

This Metasploit module creates a RAR file that exploits CVE-2022-30333, which is a path-traversal vulnerability in unRAR that can extract an arbitrary file to an arbitrary location on a Linux system. UnRAR fixed this vulnerability in version 6.12 (open source version 6.1.7). The core issue is that when a symbolic link is unRARed, Windows symbolic links are not properly validated on Linux systems and can therefore write a symbolic link that points anywhere on the filesystem. If a second file in the archive has the same name, it will be written to the symbolic link path.

- Link

—

” “Thu, 12 Sep 2024

3DSecure 2.0 3DS Authorization Method Cross Site Request Forgery

A cross site request forgery vulnerability was identified in the Authorization Method of 3DSecure version 2.0, allowing attackers to submit unauthorized form data by modifying the HTTP Origin and Referer headers.

- Link

—

” “Thu, 12 Sep 2024

3DSecure 2.0 3DS Method Authentication Cross Site Scripting

3DSecure version 2.0 is vulnerable to form action hijacking via the threeDSMethodNotificationURL parameter. This flaw allows attackers to change the destination website for form submissions, enabling data theft.

- Link

—

” “Thu, 12 Sep 2024

3DSecure 2.0 3DS Authorization Method Cross Site Scripting

Multiple reflected cross site scripting vulnerabilities in the 3DS Authorization Method of 3DSecure version 2.0 allow attackers to inject arbitrary web scripts via the threeDSMethodData parameter.

- Link

—

” “Thu, 12 Sep 2024

3DSecure 2.0 3DS Authorization Challenge Cross Site Scripting

Multiple reflected cross site scripting vulnerabilities exist in the 3DS Authorization Challenge of 3DSecure version 2.0. These flaws allow attackers to inject arbitrary web scripts, CSS, or HTML through the manipulation of the params parameter in the request URL.

- Link

—

” “Thu, 12 Sep 2024

3DSecure 2.0 3DS Method Authentication Cross Site Scripting

3DSecure version 2.0 is vulnerable to cross site scripting in its 3DSMethod Authentication. This vulnerability allows remote attackers to hijack the form action and change the destination website via the params parameter, which is base64 encoded and improperly sanitized.

- Link

—

” “Thu, 12 Sep 2024

Nipah Virus Testing Management System 1.0 PHP Code Injection

Nipah Virus Testing Management System version 1.0 suffers from a php code injection vulnerability.
- Link

—

” “Thu, 12 Sep 2024

Medical Card Generations System 1.0 SQL Injection

Medical Card Generations System version 1.0 suffers from a remote SQL injection vulnerability.
- Link

—

” “Thu, 12 Sep 2024

Maid Hiring Management System 1.0 Insecure Settings

Maid Hiring Management System version 1.0 suffers from an ignored default credential vulnerability.
- Link

—

” “Thu, 12 Sep 2024

Emergency Ambulance Hiring Portal 1.0 PHP Code Injection

Emergency Ambulance Hiring Portal version 1.0 suffers from a php code injection vulnerability.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 13 Sep 2024

ZDI-24-1226: mySCADA myPRO Hard-Coded Credentials Remote Code Execution Vulnerability
- Link

—

” “Fri, 13 Sep 2024

ZDI-24-1225: SolarWinds Access Rights Manager Hard-Coded Credentials Authentication Bypass Vulnerability
- Link

—

” “Fri, 13 Sep 2024

ZDI-24-1224: SolarWinds Access Rights Manager JsonSerializationBinder Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link

—

” “Thu, 12 Sep 2024

ZDI-24-1223: Ivanti Endpoint Manager AgentPortal Deserialization of Untrusted Data Remote

Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1222: Ivanti Workspace Control RES Exposed Dangerous Method Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1221: Ivanti Endpoint Manager LoadMotherboardTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1220: Ivanti Endpoint Manager LoadSlotsTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1219: Ivanti Endpoint Manager loadModuleTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1218: Ivanti Endpoint Manager updateAssetInfo SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1217: Ivanti Endpoint Manager loadSystemInfo SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1216: Ivanti Endpoint Manager GetSQLStatement SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1215: Ivanti Endpoint Manager loadKeyboardTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1214: Ivanti Endpoint Manager GetVulnerabilitiesDataTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1213: Ivanti Endpoint Manager loadMouseTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1212: Ivanti Endpoint Manager ImportXml XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1211: Ivanti Endpoint Manager WasPreviouslyMapped SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1210: Microsoft Windows Drag and Drop SmartScreen Bypass Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1209: Microsoft Windows Defender SmartScreen Bypass Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1208: (0Day) Visteon Infotainment System DeviceManager iAP Serial Number SQL Injection Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1207: Microsoft Windows Internet Explorer File Extension Spoofing Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1206: Microsoft SharePoint SPAutoSerializingObject Deserialization of Untrusted Data Denial-of-Service Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1205: Microsoft Windows BeginPaint Pen Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1204: Microsoft SharePoint SPThemes Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1203: Adobe Photoshop JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1202: Adobe After Effects AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1201: Adobe Premiere Pro AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1200: Adobe Media Encoder AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1199: Adobe After Effects AVI File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1198: Adobe Premiere Pro AVI File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1197: Adobe Audition AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

”

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: (Sep)

Datum	Opfer	Land	Information
2024-09-12	▯▯▯▯▯▯▯ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	Link
2024-09-09	Université de Gênes	[ITA]	Link
2024-09-08	Highline Public Schools	[USA]	Link
2024-09-08	Groupe Bayard	[FRA]	Link
2024-09-08	Isbergues	[FRA]	Link
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	Link
2024-09-05	Air-e	[COL]	Link
2024-09-05	Charles Darwin School	[GBR]	Link
2024-09-05	Elektroskandia	[SWE]	Link
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-02	Kawasaki Motors Europe	[GBR]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-13	[FD Lawrence Electric]	blacksuit	Link
2024-09-13	[True Family Enterprises]	play	Link
2024-09-13	[Dimensional Merchandising]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-13	[Creative Playthings]	play	Link
2024-09-13	[Law Offices of Michael J Gurfinkel, Inc]	bianlian	Link
2024-09-13	[Hostetler Buildings]	blacksuit	Link
2024-09-13	[VIcom Corporation]	hunters	Link
2024-09-13	[Arch-Con]	hunters	Link
2024-09-13	[HB Construction]	hunters	Link
2024-09-13	[Associated Building Specialties]	hunters	Link
2024-09-12	[www.southeasternretina.com]	ransomhub	Link
2024-09-11	[Ascend Analytics (ascendanalytics.com)]	lynx	Link
2024-09-06	[Kingsmill Resort]	qilin	Link
2024-09-12	[brunswickhospitalcenter.org]	threeam	Link
2024-09-12	[Carpenter McCadden and Lane LLP]	meow	Link
2024-09-12	[CSMR Agrupación de Colaboración Empresaria]	meow	Link
2024-09-11	[ICBC (London)]	hunters	Link
2024-09-12	[thornton-inc.com]	ransomhub	Link
2024-09-04	[nhbg.com.co]	lockbit3	Link
2024-09-12	[mechdyne.com]	ransomhub	Link
2024-09-10	[Starr-Iva Water & Sewer District]	medusa	Link
2024-09-10	[Karakaya Group]	medusa	Link
2024-09-10	[allamericanpoly.com]	ransomhub	Link
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link
2024-09-11	[Clatronic International GmbH]	fog	Link
2024-09-11	[Advanced Physician Management Services LLC]	meow	Link
2024-09-11	[Arville]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-11	[ICBC London]	hunters	Link
2024-09-11	[Ladov Law Firm]	bianlian	Link
2024-09-10	[Regent Care Center]	incransom	Link
2024-09-10	[www.vinatiorganics.com]	ransomhub	Link
2024-09-10	[Evans Distribution Systems]	play	Link
2024-09-10	[Weldco-Beales Manufacturing]	play	Link
2024-09-10	[PIGGLY WIGGLY ALABAMA DISTRIBUTING]	play	Link
2024-09-10	[Elgin Separation Solutions]	play	Link
2024-09-10	[Bel-Air Bay Club]	play	Link
2024-09-10	[Joe Swartz Electric]	play	Link
2024-09-10	[Virginia Dare Extract Co.]	play	Link
2024-09-10	[Southeast Cooler]	play	Link
2024-09-10	[IDF and Mossad agents]	meow	Link
2024-09-10	[rupicard.com]	killsec	Link
2024-09-10	[Vickers Engineering]	akira	Link
2024-09-09	[Controlled Power]	dragonforce	Link
2024-09-09	[Arc-Com]	dragonforce	Link
2024-09-10	[HDI]	bianlian	Link
2024-09-10	[Myelec Electrical]	meow	Link
2024-09-10	[Kadokawa Co Jp]	blacksuit	Link
2024-09-10	[Qeco/coeq]	rhysida	Link
2024-09-10	[E-Z Pack Holdings LLC]	incransom	Link
2024-09-10	[Bank Rakyat]	hunters	Link
2024-09-06	[americagraphics.com]	ransomhub	Link
2024-09-09	[Pennsylvania State Education Association]	rhysida	Link
2024-09-09	[Anniversary Holding]	bianlian	Link
2024-09-09	[Battle Lumber Co.]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[Appellation vins fins]	ransomhub	Link
2024-09-09	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link
2024-09-09	[pv.be]	killsec	Link
2024-09-09	[Smart Source, Inc.]	bianlian	Link
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	Link
2024-09-06	[□□□□□□□□]	cicada3301	Link
2024-09-08	[Stratford School Academy]	rhysida	Link
2024-09-07	[cardiovirginia.com]	ransomhub	Link
2024-09-07	[Prosolit]	medusa	Link
2024-09-07	[Grupo Cortefiel]	medusa	Link
2024-09-07	[Nocciole Marchisio]	meow	Link
2024-09-07	[Elsoms Seeds]	meow	Link
2024-09-07	[Millsboro Animal Hospital]	qilin	Link
2024-09-05	[briedis.lt]	ransomhub	Link
2024-09-06	[America Voice]	medusa	Link
2024-09-06	[CK Associates]	bianlian	Link
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	Link
2024-09-06	[ctelift.com]	madliberator	Link
2024-09-06	[SESAM Informatics]	hunters	Link
2024-09-06	[riomarineinc.com]	cactus	Link
2024-09-06	[champeau.com]	cactus	Link
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link
2024-09-05	[dvv.be]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[Custom Security Systems]	hunters	Link
2024-09-05	[Inglenorth.co.uk]	ransomhub	Link
2024-09-05	[cps-k12.org]	ransomhub	Link
2024-09-05	[inorde.com]	ransomhub	Link
2024-09-05	[tri-tech.us]	ransomhub	Link
2024-09-05	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link
2024-09-05	[phdservices.net]	ransomhub	Link
2024-09-05	[cbt-gmbh.de]	ransomhub	Link
2024-09-05	[www.towellengineering.net]	ransomhub	Link
2024-09-04	[rhp.com.br]	lockbit3	Link
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	Link
2024-09-05	[Imetame]	akira	Link
2024-09-05	[SWISS CZ]	akira	Link
2024-09-05	[Cellular Plus]	akira	Link
2024-09-05	[Arch Street Capital Advisors]	qilin	Link
2024-09-04	[Hospital Episcopal San Lucas]	medusa	Link
2024-09-05	[www.parknfly.ca]	ransomhub	Link
2024-09-05	[Western Supplies, Inc]	bianlian	Link
2024-09-04	[Farmers' Rice Cooperative]	play	Link
2024-09-04	[Bakersfield]	play	Link
2024-09-04	[Crain Group]	play	Link
2024-09-04	[Parrish]	blacksuit	Link
2024-09-04	[www.galgorm.com]	ransomhub	Link
2024-09-04	[www.pcipa.com]	ransomhub	Link
2024-09-04	[ych.com]	madliberator	Link
2024-09-04	[www.bennettcurrie.co.nz]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	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
2024-09-02	[Kingsport Imaging Systems]	medusa	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
2024-09-01	[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.