Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240923

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

Jetzt patchen! Attacken auf Ivanti Cloud Service Appliance verschärfen sich

Derzeit kombinieren Angreifer zwei Sicherheitslücken, um auf Cloud Services Appliances von Ivanti Schadcode auszuführen.

- Link

—

Kritische SAML-Anmelde-Lücke mit Höchstwertung gefährdet Gitlab-Server

Unter bestimmten Voraussetzungen können sich Angreifer Zugriff auf die DevSecOps-Plattform Gitlab verschaffen.

- Link

—

Sicherheitsupdates: BIOS-Lücken gefährden Dell-Computer

Unter anderem sind bestimmte Computer von Dells Alienware-Serie attackierbar. Sicherheitspatches stehen zum Download.

- Link

—

Sicherheitslücken: Netzwerk-Controller und -Gateways von Aruba sind verwundbar

Angreifer können Netzwerkgeräte von HPE Aruba attackieren und im schlimmsten Fall Appliances kompromittieren.

- Link

—

VMware vCenter: Angreifer aus dem Netz können Schadcode einschleusen

Broadcom stopft mehrere Sicherheitslücken in VMware vCenter. Schlimmstenfalls können Angreifer aus dem Netz Schadcode einschmuggeln und ausführen.

- Link

—

Samsung-Druckertreiber ermöglichen Angreifern Rechteausweitung

Für Samsungs Office-Drucker stellt HP einen aktualisierten Universal-Treiber für Windows bereit. Er dichtet ein Rechteausweitungsleck ab.

- Link

—

Angreifer attackieren Sicherheitslücken in Microsofts MSHTML und Whatsup Gold

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt vor Angriffen auf Sicherheitslücken in Microsofts MSHTML und Whatsup Gold.

- Link

—

Sicherheitspatch: Hintertür in einigen D-Link-Routern erlaubt unbefugte Zugriffe

Angreifer können bestimmte Router-Modelle von D-Link attackieren und kompromittieren. Sicherheitsupdates stehen zum Download bereit.

- Link

—

Sicherheitspatch verfügbar: Angriffe auf Ivanti Cloud Service Appliance

Derzeit attackieren Angreifer Ivanti Cloud Service Appliances mit Schadcode. Außedem könnten Attacken auf Endpoint Manager bevorstehen.

- Link

—

Lenovo schließt Lücken in BIOS, Management-Controller und WLAN-Treiber

Wichtige Sicherheitsupdates schützen Computer von Lenovo. Im schlimmsten Fall können Angreifer Schadcode ausführen.

- 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	0.994730000	Link
CVE-2023-6895	0.927330000	0.990690000	Link
CVE-2023-6553	0.947820000	0.993110000	Link
CVE-2023-6019	0.918710000	0.989900000	Link
CVE-2023-52251	0.945480000	0.992740000	Link
CVE-2023-4966	0.970840000	0.998150000	Link
CVE-2023-49103	0.949680000	0.993430000	Link
CVE-2023-48795	0.964670000	0.996220000	Link
CVE-2023-47246	0.961220000	0.995430000	Link
CVE-2023-46805	0.950230000	0.993520000	Link
CVE-2023-46747	0.971020000	0.998240000	Link
CVE-2023-46604	0.969070000	0.997520000	Link
CVE-2023-4542	0.948590000	0.993230000	Link
CVE-2023-43208	0.973740000	0.999270000	Link
CVE-2023-43177	0.961480000	0.995490000	Link
CVE-2023-42793	0.972380000	0.998700000	Link
CVE-2023-41265	0.907590000	0.989130000	Link
CVE-2023-39143	0.940700000	0.992190000	Link
CVE-2023-38205	0.949280000	0.993350000	Link
CVE-2023-38203	0.965830000	0.996580000	Link
CVE-2023-38146	0.919150000	0.989950000	Link
CVE-2023-38035	0.974550000	0.999650000	Link
CVE-2023-36845	0.967850000	0.997160000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996610000	Link
CVE-2023-35082	0.966710000	0.996830000	Link
CVE-2023-35078	0.971130000	0.998280000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.900520000	0.988690000	Link
CVE-2023-34634	0.923140000	0.990300000	Link
CVE-2023-34362	0.970450000	0.997980000	Link
CVE-2023-34039	0.945100000	0.992690000	Link
CVE-2023-3368	0.939780000	0.992080000	Link
CVE-2023-33246	0.967830000	0.997150000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953820000	0.994180000	Link
CVE-2023-30013	0.965950000	0.996620000	Link
CVE-2023-29300	0.967820000	0.997150000	Link
CVE-2023-29298	0.969390000	0.997610000	Link
CVE-2023-28432	0.920500000	0.990070000	Link
CVE-2023-28343	0.937460000	0.991780000	Link
CVE-2023-28121	0.922260000	0.990240000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.974150000	0.999480000	Link
CVE-2023-27350	0.969520000	0.997640000	Link
CVE-2023-26469	0.953540000	0.994120000	Link
CVE-2023-26360	0.964390000	0.996130000	Link
CVE-2023-26035	0.968720000	0.997400000	Link
CVE-2023-25717	0.950620000	0.993570000	Link
CVE-2023-25194	0.965150000	0.996380000	Link
CVE-2023-2479	0.963230000	0.995850000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.973150000	0.999040000	Link
CVE-2023-23752	0.951460000	0.993690000	Link
CVE-2023-23333	0.960430000	0.995240000	Link
CVE-2023-22527	0.970940000	0.998200000	Link
CVE-2023-22518	0.957870000	0.994840000	Link
CVE-2023-22515	0.973160000	0.999070000	Link
CVE-2023-21839	0.947720000	0.993090000	Link
CVE-2023-21554	0.952650000	0.993970000	Link
CVE-2023-20887	0.970840000	0.998140000	Link
CVE-2023-1671	0.962220000	0.995630000	Link
CVE-2023-0669	0.971300000	0.998350000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 20 Sep 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, beliebigen Code auszuführen oder nicht spezifizierte Effekte zu erzielen.

- Link

—

Fri, 20 Sep 2024

[NEU] [hoch] FreeBSD Project FreeBSD OS: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in FreeBSD Project FreeBSD OS ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] CoreDNS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CoreDNS ausnutzen, um einen

Denial of Service Angriff durchzuführen oder ein DNS-Cache-Poisoning durchzuführen.

- Link

—

Fri, 20 Sep 2024

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

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

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- Link

—

Fri, 20 Sep 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

—

Fri, 20 Sep 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung und DoS

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 20 Sep 2024

[UPDATE] [hoch] Microsoft Azure: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 20 Sep 2024

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

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

- Link

—

Fri, 20 Sep 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

—

Fri, 20 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, 20 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

—

Fri, 20 Sep 2024

[UPDATE] [hoch] FreeBSD Project FreeBSD OS: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Codeausführung

Ein Angreifer kann mehrere Schwachstellen in FreeBSD Project FreeBSD OS ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.
- Link

—

Fri, 20 Sep 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Wireshark: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Wireshark ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link

—

Thu, 19 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

—

Thu, 19 Sep 2024

[UPDATE] [kritisch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/22/2024	[GLSA-202409-14 : Mbed TLS: Multiple Vulnerabilities]	critical
9/22/2024	[GLSA-202409-01 : Portage: Unverified PGP Signatures]	critical
9/22/2024	[GLSA-202409-12 : pypy, pypy3: Multiple Vulnerabilities]	critical
9/22/2024	[GLSA-202409-08 : OpenVPN: Multiple Vulnerabilities]	critical
9/22/2024	[GLSA-202409-16 : Slurm: Multiple Vulnerabilities]	critical
9/22/2024	[GLSA-202409-19 : Emacs, org-mode: Command Execution Vulnerability]	critical
9/21/2024	[Fedora 39 : expat (2024-527052ab76)]	critical
9/21/2024	[FreeBSD : FreeBSD – bhyve(8) out-of-bounds read access via XHCI emulation (1febd09b-7716-11ef-9a62-002590c1f29c)]	critical
9/20/2024	[AlmaLinux 8 : thunderbird (ALSA-2024:6684)]	critical
9/20/2024	[Debian dsa-5774 : ruby-saml - security update]	critical
9/20/2024	[AlmaLinux 9 : firefox (ALSA-2024:6681)]	critical
9/20/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:6683)]	critical
9/22/2024	[Fedora 39 : less (2024-c94f884440)]	high
9/22/2024	[Fedora 39 : chromium (2024-3d29b1647b)]	high
9/22/2024	[GLSA-202409-10 : Xen: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-15 : stb: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-03 : GPL Ghostscript: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-05 : PJSIP: Heap Buffer Overflow]	high
9/22/2024	[GLSA-202409-11 : Oracle VirtualBox: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-02 : PostgreSQL: Privilege Escalation]	high
9/22/2024	[GLSA-202409-09 : Exo: Arbitrary Code Execution]	high
9/22/2024	[GLSA-202409-13 : gst-plugins-good: Multiple Vulnerabilities]	high

Datum	Schwachstelle	Bewertung
9/22/2024	[GLSA-202409-04 : calibre: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-07 : Rust: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-18 : liblouis: Multiple Vulnerabilities]	high
9/22/2024	[GLSA-202409-17 : VLC: Multiple Vulnerabilities]	high
9/21/2024	[Fedora 39 : aardvark-dns (2024-0ce77b8571)]	high
9/21/2024	[SUSE SLES15 Security Update : kernel (Live Patch 15 for SLE 15 SP5) (SUSE-SU-2024:3350-1)]	high
9/21/2024	[SUSE SLES15 / openSUSE 15 Security Update : python310 (SUSE-SU-2024:3357-1)]	high
9/21/2024	[FreeBSD : FreeBSD – Integer overflow in libnv (93c12fe5-7716-11ef-9a62-002590c1f29c)]	high
9/21/2024	[FreeBSD : FreeBSD – pf incorrectly matches different ICMPv6 states in the state table (f140cff0-771a-11ef-9a62-002590c1f29c)]	high
9/21/2024	[FreeBSD : FreeBSD – ktrace(2) fails to detach when executing a setuid binary (8fb61d94-771b-11ef-9a62-002590c1f29c)]	high
9/21/2024	[CBL Mariner 2.0 Security Update: xorg-x11-server (CVE-2024-0229)]	high
9/21/2024	[CBL Mariner 2.0 Security Update: libxml2 (CVE-2024-25062)]	high
9/21/2024	[CBL Mariner 2.0 Security Update: xorg-x11-server (CVE-2024-0409)]	high
9/21/2024	[CBL Mariner 2.0 Security Update: xorg-x11-server (CVE-2024-21886)]	high
9/21/2024	[Oracle Linux 8 : libreoffice (ELSA-2024-5598)]	high
9/21/2024	[Oracle Linux 9 : libreoffice (ELSA-2024-5583)]	high
9/20/2024	[AlmaLinux 9 : libnbd (ALSA-2024:6757)]	high
9/20/2024	[AlmaLinux 8 : ruby:3.3 (ALSA-2024:6784)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 20 Sep 2024

BlackNET 3.7.0.0 Missing Authentication / File Deletion / Traversal

BlackNET version 3.7.0.0 appears to allow unauthenticated access to modify data and suffers from arbitrary file deletion and directory traversal vulnerabilities while authenticated.

- Link

—

” “Fri, 20 Sep 2024

SPIP BigUp 4.2.15 Code Injection

SPIP BigUp version 4.2.15 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Fri, 20 Sep 2024

Taskhub 3.0.3 Insecure Settings

Taskhub version 3.0.3 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 20 Sep 2024

Teacher Subject Allocation Management System 1.0 Cross Site Scripting

Teacher Subject Allocation Management System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 20 Sep 2024

Transport Management System 1.0 SQL Injection

Transport Management System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 20 Sep 2024

Travel Management System Project 1.0 Arbitrary File Upload

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

- Link

—

” “Fri, 20 Sep 2024

Vaidya-Mitra 1.0 Cross Site Request Forgery

Vaidya-Mitra version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Fri, 20 Sep 2024

Online Food Management System 1.0 Insecure Direct Object Reference

Online Food Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Thu, 19 Sep 2024

htmly 2.9.9 Cross Site Scripting

htmly version 2.9.9 suffers from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Thu, 19 Sep 2024

WordPress LMS 4.2.7 SQL Injection

WordPress LMS plugin versions 4.2.7 and below suffer from a remote SQL injection vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Nexus Repository Manager 3 Path Traversal

Proof of concept exploit that demonstrates an unauthenticated path traversal vulnerability in Nexus Repository Manager version 3.

- Link

—

” “Thu, 19 Sep 2024

Check Point Security Gateways Information Disclosure

Proof of concept exploit that demonstrates an information disclosure vulnerability in Check Point Security Gateways.

- Link

—

” “Thu, 19 Sep 2024

Telerik Report Server 2024 Q1 Authentication Bypass

In Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier, on IIS, an unauthenticated attacker can gain access to Telerik Report Server restricted functionality via an authentication bypass vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Prison Management System 1.0 Code Injection

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

- Link

—

” “Thu, 19 Sep 2024

PreSchool Enrollment System 1.0 SQL Injection

PreSchool Enrollment System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 19 Sep 2024

SchoolPlus 1.0 Cross Site Request Forgery

SchoolPlus version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Security Guard Hiring System 1.0 Insecure Settings

Online Security Guard Hiring System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Food Management System 1.0 SQL Injection

Online Food Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 19 Sep 2024

SPIP BigUp 4.1.17 Code Injection

SPIP BigUp version 4.1.17 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Exam System 1.0 Information Disclosure

Online Exam System version 1.0 suffers from an information disclosure vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Old Age Home Management System 1.0 Insecure Settings

Old Age Home Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Nipah Virus Testing Management System 1.0 Insecure Settings

Nipah Virus Testing Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Men Salon Management System 2.0 Insecure Settings

Men Salon Management System version 2.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Online Traffic Offense 1.0 CSRF / Arbitrary File Upload

Online Traffic Offense version 1.0 suffers from cross site request forgery and arbitrary file upload vulnerabilities.

- Link

—

” “Wed, 18 Sep 2024

Backdoor.Win32.CCInvader.10 MVID-2024-0694 Authentication Bypass

Backdoor.Win32.CCInvader.10 malware suffers from a bypass 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: (Sep)

Datum	Opfer	Land	Information
2024-09-16	TAAG	[AGO]	Link
2024-09-16	Heinrich-Böll-Gesamtschule et Rurtal-Gymnasium	[DEU]	Link
2024-09-16	Fylde Coast Academy Trust	[GBR]	Link
2024-09-15	Radio Geretsried	[DEU]	Link
2024-09-15	Technet	[NOR]	Link
2024-09-14	Zacros	[JPN]	Link
2024-09-12	⊠⊠⊠⊠⊠⊠ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	Link
2024-09-11	Providence Public School District (PPSD)	[USA]	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
2024-09-04	Compass Group	[AUS]	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
2024-09-23	[Canstar Restorations]	qilin	Link
2024-09-22	[hanwa.co.th]	BrainCipher	Link
2024-09-22	[Daughterly Care]	rhysida	Link
2024-09-22	[Woodard , Hernandez , Roth & Day]	qilin	Link
2024-09-21	[savannahcandy.com]	ransomhub	Link
2024-09-21	[Acho.io]	ransomhub	Link
2024-09-05	[Bayou DeSiard Country Club]	cicada3301	Link
2024-09-20	[Jackson Paper Manufacturing]	play	Link
2024-09-20	[Messe C]	play	Link
2024-09-20	[Noble Environmental]	play	Link
2024-09-20	[Omega Industries]	play	Link
2024-09-20	[Pacific Coast Building Products]	play	Link
2024-09-20	[Thompson Construction Supply]	play	Link
2024-09-20	[Visionary Homes]	incransom	Link
2024-09-20	[KW Realty Group]	qilin	Link
2024-09-20	[Capital Printing]	cicada3301	Link
2024-09-18	[virainsight.com]	ransomhub	Link
2024-09-20	[Juice Generation]	fog	Link
2024-09-20	[River Region Cardiology Associates]	bianlian	Link
2024-09-20	[Greene Acres Nursing Home]	rhysida	Link
2024-09-20	[aroma.com.tr]	ransomhub	Link
2024-09-19	[rarholding.com]	ransomhub	Link
2024-09-19	[Fritzøe Engros]	medusa	Link
2024-09-19	[Wilson & Lafleur]	medusa	Link
2024-09-19	[Wertachkliniken.de]	cloak	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-19	[newriverelectrical.com]	ElDorado	Link
2024-09-19	[seaglesafety.com]	ElDorado	Link
2024-09-19	[rccauto.com]	ElDorado	Link
2024-09-19	[itasnatta.edu.it]	ElDorado	Link
2024-09-19	[a1mobilelock.com]	ElDorado	Link
2024-09-19	[curvc.com]	ElDorado	Link
2024-09-19	[patricksanderscompany.com]	ElDorado	Link
2024-09-19	[thinksimple.com]	ElDorado	Link
2024-09-19	[pesprograms.com]	ElDorado	Link
2024-09-19	[palmfs.com]	ElDorado	Link
2024-09-19	[kennedyfunding.com]	ElDorado	Link
2024-09-19	[advbe.com]	ransomhub	Link
2024-09-19	[Sunrise Farms]	fog	Link
2024-09-19	[Nusser Mineralöl GmbH]	incransom	Link
2024-09-19	[avl1.com]	ransomhub	Link
2024-09-19	[libertyfirstcu.com]	ransomhub	Link
2024-09-19	[Hunter Dickinson Inc.]	bianlian	Link
2024-09-19	[tims.com]	abyss	Link
2024-09-18	[bspcr.com]	lockbit3	Link
2024-09-18	[lakelandchamber.com]	lockbit3	Link
2024-09-18	[yesmoke.eu]	lockbit3	Link
2024-09-18	[efile.com]	lockbit3	Link
2024-09-18	[paybito.com]	lockbit3	Link
2024-09-18	[Compass Group (2nd attack)]	medusa	Link
2024-09-18	[Structural Concepts]	medusa	Link
2024-09-19	[Vidisco]	handala	Link
2024-09-19	[IIB (Israeli Industrial Batteries)]	handala	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-18	[Plaisted Companies]	play	Link
2024-09-11	[Bertelkamp Automation]	qilin	Link
2024-09-18	[DJH Jugendherberge]	hunters	Link
2024-09-18	[Prentke Romich Company]	fog	Link
2024-09-12	[agricola]	qilin	Link
2024-09-16	[Amerinational Community Services]	medusa	Link
2024-09-16	[Providence Public School Department]	medusa	Link
2024-09-16	[AZPIRED]	medusa	Link
2024-09-17	[Compass Group]	medusa	Link
2024-09-18	[Chernan Technology]	orca	Link
2024-09-18	[Port of Seattle/Seattle-Tacoma International Airport (SEA)]	rhysida	Link
2024-09-16	[Baskervill]	play	Link
2024-09-16	[Protective Industrial Products]	play	Link
2024-09-16	[Inktel]	play	Link
2024-09-16	[Rsp]	play	Link
2024-09-16	[Hariri Pontarini Architects]	play	Link
2024-09-16	[Multidata]	play	Link
2024-09-18	[Environmental Code Consultants Inc]	meow	Link
2024-09-18	[EnviroNET Inc]	meow	Link
2024-09-18	[Robson Planning Group Inc]	meow	Link
2024-09-16	[oipip.gda.pl]	ransomhub	Link
2024-09-16	[kryptonresources.com]	ransomhub	Link
2024-09-16	[www.tta.cls]	ransomhub	Link
2024-09-18	[globe.com.bd]	ValenciaLeaks	Link
2024-09-18	[satiagroup.com]	ValenciaLeaks	Link
2024-09-18	[duopharmabiotech.com]	ValenciaLeaks	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-18	[tendam.es]	ValenciaLeaks	Link
2024-09-18	[cityofpleasantonca.gov]	ValenciaLeaks	Link
2024-09-16	[www.faithfc.org]	ransomhub	Link
2024-09-16	[www.adantia.es]	ransomhub	Link
2024-09-16	[topdoctors.com]	ransomhub	Link
2024-09-16	[www.8010urbanliving.com]	ransomhub	Link
2024-09-16	[www.taperuvicha.com]	ransomhub	Link
2024-09-17	[www.plumbersstock.com]	ransomhub	Link
2024-09-17	[www.nikpol.com.au]	ransomhub	Link
2024-09-18	[www.galloway-macleod.co.uk]	ransomhub	Link
2024-09-18	[ringpower.com]	ransomhub	Link
2024-09-17	[miit.gov.cn]	killsec	Link
2024-09-17	[New Electric]	hunters	Link
2024-09-17	[AutoCanada]	hunters	Link
2024-09-17	[natcoglobal.com]	cactus	Link
2024-09-17	[Sherr Puttmann Akins Lamb PC]	bianlian	Link
2024-09-17	[peerlessumbrella.com]	cactus	Link
2024-09-17	[thomas-lloyd.com]	cactus	Link
2024-09-16	[Cruz Marine (cruz.local)]	lynx	Link
2024-09-16	[SuperCommerce.ai]	killsec	Link
2024-09-16	[MCNA Dental 1 million patients records]	everest	Link
2024-09-16	[ExcelPlast Tunisie]	orca	Link
2024-09-16	[northernsafety.com]	blackbasta	Link
2024-09-16	[thompsoncreek.com]	blackbasta	Link
2024-09-07	[www.atlcc.net]	ransomhub	Link
2024-09-10	[accurateraillroad.com]	ransomhub	Link
2024-09-10	[advantagecdc.org]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-10	[lafuturasrl.it]	ransomhub	Link
2024-09-15	[dowley.com]	lockbit3	Link
2024-09-15	[apexbrasil.com.br]	lockbit3	Link
2024-09-15	[fivestarproducts.com]	lockbit3	Link
2024-09-15	[ignitarium.com]	lockbit3	Link
2024-09-15	[nfcaa.org]	lockbit3	Link
2024-09-15	[Emtel]	arcusmedia	Link
2024-09-15	[salaam.af]	lockbit3	Link
2024-09-15	[INTERNAL.ROCKYMOUNTAINGASTRO.COM]	trinity	Link
2024-09-14	[Gino Giglio Generation Spa]	arcusmedia	Link
2024-09-14	[Rextech]	arcusmedia	Link
2024-09-14	[Like Family's]	arcusmedia	Link
2024-09-14	[UNI-PA A.Ş]	arcusmedia	Link
2024-09-12	[OnePoint Patient Care]	incransom	Link
2024-09-14	[Retemex]	ransomexx	Link
2024-09-14	[ORCHID-ORTHO.COM]	clop	Link
2024-09-11	[jatelindo]	stormous	Link
2024-09-13	[mivideo.club]	stormous	Link
2024-09-12	[Micron Internet]	medusa	Link
2024-09-12	[TECHNOLOG S.r.l.]	medusa	Link
2024-09-14	[ecbawm.com]	abyss	Link
2024-09-13	[FD Lawrence Electric]	blacksuit	Link
2024-09-13	[True Family Enterprises]	play	Link
2024-09-13	[Dimensional Merchandising]	play	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-12	[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
2024-09-11	[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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[Appellation vins fins]	ransomhub	Link
2024-09-07	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[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
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	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-01	[cbt-gmbh.de]	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
2024-09-03	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.