Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240129

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

Schadcode-Attacken auf Onlineshops auf Gambio-Basis möglich

Admins von Onlineshops sollten die Gambio-Software aus Sicherheitsgründen auf den aktuellen Stand bringen.

- Link

—

Diesmal bitte patchen: Security-Update behebt kritische Schwachstelle in GitLab

GitLab 16.x enthält fünf Schwachstellen, von denen eine als kritisch eingestuft ist. Patchen ist nicht selbstverständlich, wie jüngst eine Untersuchung zeigte.

- Link

—

Microsoft Edge 121 unterstützt moderne Codecs und stopft Sicherheitslecks

Microsoft hat den Webbrowser Edge in Version 121 herausgegeben. Sie stopft eine kritische Sicherheitslücke und liefert Support für AV1-Videos.

- Link

—

Angreifer können eigene Befehle auf Juniper-Firewalls und Switches ausführen

Entwickler von Juniper haben in Junos OS mehrere Sicherheitslücken geschlossen. Noch sind aber nicht alle Updates verfügbar.

- Link

—

Automatisierungstool Jenkins: Codeschmuggel durch Sicherheitslücke möglich

Sicherheitslücken in der Open-Source-Automatisierungssoftware Jenkins erlauben Angreifern, Schadcode einzuschmuggeln. Updates helfen dem ab.

- Link

—

Cisco: Lücke erlaubt komplette Übernahme von Unified Communication-Produkten

Cisco warnt vor einer kritischen Lücke in Unified Communication-Produkten, durch die Angreifer die Kontrolle übernehmen können.

- Link

—

Gitlab-Kontoklau-Lücke: Tausende verwundbare Server im Netz

IT-Forscher haben das Netz durchforstet und dabei mehr als 5000 verwundbare Gitlab-Server gefunden. Angreifer können dort einfach Konten übernehmen.

- Link

—

Trend Micro Apex Central: Update schließt im zweiten Anlauf Sicherheitslücken

Mehrere Sicherheitslücken in Trend Micros Apex Central ermöglichen Angreifern etwa, Schadcode einzuschleusen. Ein erstes Update machte Probleme.

- Link

—

Codeschmuggel-Lücke in HPE Oneview

Mehrere Sicherheitslücken in der IT-Infrastrukturverwaltung HPE Oneview ermöglichen Angreifern, etwa Schadcode einzuschleusen. Updates stehen bereit.

- Link

—

Firefox: Passkey-Unterstützung und Sicherheitsfixes

Die Version 122 von Firefox kann mit Passkeys umgehen. Außerdem schließen die Entwickler darin wie in Firefox ESR und Thunderbird 115.7 Sicherheitslecks.

- 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-2023-6553	0.909010000	0.986320000	Link
CVE-2023-5360	0.967230000	0.995890000	Link
CVE-2023-4966	0.931240000	0.988770000	Link
CVE-2023-46805	0.930450000	0.988690000	Link
CVE-2023-46747	0.965530000	0.995290000	Link
CVE-2023-46604	0.971470000	0.997630000	Link
CVE-2023-42793	0.973260000	0.998690000	Link
CVE-2023-38035	0.971870000	0.997820000	Link
CVE-2023-35082	0.932740000	0.989040000	Link
CVE-2023-35078	0.953380000	0.992130000	Link
CVE-2023-34634	0.906880000	0.986070000	Link
CVE-2023-34362	0.954180000	0.992310000	Link
CVE-2023-33246	0.971270000	0.997540000	Link
CVE-2023-32315	0.963290000	0.994480000	Link
CVE-2023-30625	0.937630000	0.989540000	Link
CVE-2023-30013	0.925700000	0.988160000	Link
CVE-2023-29300	0.939750000	0.989800000	Link
CVE-2023-28771	0.923800000	0.987910000	Link
CVE-2023-27524	0.961820000	0.994020000	Link
CVE-2023-27372	0.969410000	0.996710000	Link
CVE-2023-27350	0.972430000	0.998170000	Link
CVE-2023-26469	0.927230000	0.988340000	Link
CVE-2023-26360	0.943910000	0.990440000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-26035	0.968710000	0.996470000	Link
CVE-2023-25717	0.956130000	0.992760000	Link
CVE-2023-25194	0.916080000	0.986960000	Link
CVE-2023-2479	0.958820000	0.993340000	Link
CVE-2023-24489	0.968380000	0.996320000	Link
CVE-2023-23752	0.963140000	0.994410000	Link
CVE-2023-22527	0.970540000	0.997160000	Link
CVE-2023-22518	0.965250000	0.995140000	Link
CVE-2023-22515	0.956820000	0.992910000	Link
CVE-2023-21839	0.957980000	0.993140000	Link
CVE-2023-21823	0.940060000	0.989850000	Link
CVE-2023-21554	0.961220000	0.993840000	Link
CVE-2023-20887	0.962660000	0.994230000	Link
CVE-2023-20198	0.921510000	0.987560000	Link
CVE-2023-1671	0.953130000	0.992080000	Link
CVE-2023-0669	0.968210000	0.996270000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 26 Jan 2024

[NEU] [hoch] Juniper JUNOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Juniper JUNOS, Juniper SRX Series und Juniper EX Series ausnutzen, um Informationen offenzulegen und einen Cross-Site-Scripting Angriff auszuführen.

- Link

—

Fri, 26 Jan 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Informationen falsch darzustellen und nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Fri, 26 Jan 2024

[NEU] [UNGEPATCHT] [hoch] Symantec Data Loss Prevention: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Symantec Data Loss Prevention ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Jenkins: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 26 Jan 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um beliebigen Programmcode auszuführen, unbekannte Auswirkungen zu verursachen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen

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

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] TLS: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in TLS 1.2 ausnutzen, um Sicher-

heitsvorkehrungen zu umgehen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service

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

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- Link

—

Fri, 26 Jan 2024

[NEU] [hoch] Red Hat Enterprise Linux Quarkus: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red

Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen und vertrauliche Informationen offenzulegen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Offenlegung von Informationen

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um Informationen offenzulegen und einen Denial of Service Zustand herzustellen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Android Patchday Juni 2022

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand auszulösen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- Link

—

Fri, 26 Jan 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/28/2024	[Debian dsa-5609 : libpam-slurm - security update]	critical
1/27/2024	[FreeBSD : Gitlab – vulnerabilities (61fe903b-bc2e-11ee-b06e-001b217b3468)]	critical
1/27/2024	[SUSE SLES15 / openSUSE 15 Security Update : sevctl (SUSE-SU-2024:0250-1)]	critical
1/27/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:0242-1)]	critical
1/27/2024	[Debian dsa-5608 : gir1.2-gst-plugins-bad-1.0 - security update]	critical
1/26/2024	[EulerOS 2.0 SP11 : perl (EulerOS-SA-2024-1110)]	critical
1/26/2024	[EulerOS 2.0 SP11 : perl (EulerOS-SA-2024-1126)]	critical
1/28/2024	[Fedora 39 : sudo (2024-cdccda4f62)]	high
1/27/2024	[SUSE SLED15 / SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:0252-1)]	high

Datum	Schwachstelle	Bewertung
1/27/2024	[SUSE SLES12 Security Update : jasper (SUSE-SU-2024:0240-1)]	high
1/27/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : jasper (SUSE-SU-2024:0241-1)]	high
1/27/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xorg-x11-server (SUSE-SU-2024:0249-1)]	high
1/27/2024	[SUSE SLED15 / SLES15 Security Update : xorg-x11-server (SUSE-SU-2024:0251-1)]	high
1/26/2024	[EulerOS 2.0 SP11 : python-pillow (EulerOS-SA-2024-1128)]	high
1/26/2024	[EulerOS 2.0 SP11 : kernel (EulerOS-SA-2024-1107)]	high
1/26/2024	[EulerOS 2.0 SP11 : haproxy (EulerOS-SA-2024-1106)]	high
1/26/2024	[EulerOS 2.0 SP11 : python-cryptography (EulerOS-SA-2024-1127)]	high
1/26/2024	[EulerOS 2.0 SP11 : xorg-x11-server (EulerOS-SA-2024-1115)]	high
1/26/2024	[EulerOS 2.0 SP11 : xorg-x11-server (EulerOS-SA-2024-1131)]	high
1/26/2024	[EulerOS 2.0 SP11 : python-pillow (EulerOS-SA-2024-1112)]	high
1/26/2024	[EulerOS 2.0 SP11 : python-cryptography (EulerOS-SA-2024-1111)]	high
1/26/2024	[EulerOS 2.0 SP11 : kernel (EulerOS-SA-2024-1122)]	high
1/26/2024	[EulerOS 2.0 SP11 : haproxy (EulerOS-SA-2024-1121)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 26 Jan 2024

Vinchin Backup And Recovery 7.2 SystemHandler.class.php Command Injection

Vinchin Backup and Recovery versions 7.2 and below suffer from a command injection vulnerability in SystemHandler.class.php.

- Link

—

” “Fri, 26 Jan 2024

Vinchin Backup And Recovery 7.2 Default Root Credentials

Vinchin Backup and Recovery version 7.2 has been identified as being configured with default root credentials, posing a significant security vulnerability.

- Link

—

” “Fri, 26 Jan 2024

Vinchin Backup And Recovery 7.2 Default MySQL Credentials

A critical security issue has been discovered in Vinchin Backup and Recovery version 7.2. The software has been found to use default MYSQL credentials, which could lead to significant security risks.

- Link

—

” “Fri, 26 Jan 2024

Vinchin Backup And Recovery 7.2 syncNtpTime Command Injection

Vinchin Backup and Recovery versions 7.2 and below suffer from a command injection vulnerability in the syncNtpTime function.

- Link

—

” “Fri, 26 Jan 2024

CloudLinux CageFS 7.0.8-2 Insufficiently Restricted Proxy Command

CloudLinux CageFS versions 7.0.8-2 and below insufficiently restrict file paths supplied to the sendmail proxy command. This allows local users to read and write arbitrary files of certain file formats outside the CageFS environment.

- Link

—

” “Fri, 26 Jan 2024

CloudLinux CageFS 7.1.1-1 Token Disclosure

CloudLinux CageFS versions 7.1.1-1 and below pass the authentication token as a command line argument. In some configurations this allows local users to view the authentication token via the process list and gain code execution as another user.

- Link

—

” “Fri, 26 Jan 2024

Atlassian Confluence SSTI Injection

This Metasploit module exploits an SSTI injection in Atlassian Confluence servers. A specially crafted HTTP request uses the injection to evaluate an OGNL expression resulting in OS command execution. Versions 8.5.0 through 8.5.3 and 8.0 to 8.4 are known to be vulnerable.

- Link

—

” “Fri, 26 Jan 2024

Vinchin Backup And Recovery 7.2 setNetworkCardInfo Command Injection

Vinchin Backup and Recovery versions 7.2 and below suffer from a command injection vulnerability in the setNetworkCardInfo function.

- Link

—

” “Fri, 26 Jan 2024

YahooPOPs 1.6 Denial Of Service

YahooPOPs version 1.6 remote denial of service exploit.

- Link

—

” “Fri, 26 Jan 2024

Chrome content::NavigationURLLoaderImpl::FallbackToNonInterceptedRequest Heap Use-After-Free

Chrome suffers from a heap use-after-free vulnerability in content::NavigationURLLoaderImpl::FallbackToNonIntercep

- Link

—

” “Thu, 25 Jan 2024

Gabriels FTP Server 1.2 Denial Of Service

Gabriels FTP Server version 1.2 remote denial of service exploit.

- Link

—

” “Wed, 24 Jan 2024

GL.iNet Unauthenticated Remote Command Execution

A command injection vulnerability exists in multiple GL.iNet network products, allowing an attacker to inject and execute arbitrary shell commands via JSON parameters at the gl_system_log and gl_crash_log interface in the logread module. This Metasploit exploit requires post-authentication using the Admin-Token cookie/sessionID (SID), typically stolen by the attacker. However, by chaining this exploit with vulnerability CVE-2023-50919, one can bypass the Nginx authentication through a Lua string pattern matching and SQL injection vulnerability. The Admin-Token cookie/SID can be retrieved without knowing a valid username and password. Many products are vulnerable.

- Link

—

” “Wed, 24 Jan 2024

Saltstack Minion Payload Deployer

This Metasploit exploit module uses saltstack salt to deploy a payload and run it on all targets which

have been selected (default all). Currently only works against nix targets.

- Link

—

” “Wed, 24 Jan 2024

Employee Management System 1.0 SQL Injection

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

- Link

—

” “Wed, 24 Jan 2024

MiniWeb HTTP Server 0.8.19 Denial Of Service

MiniWeb HTTP Server version 0.8.19 remote denial of service exploit.

- Link

—

” “Wed, 24 Jan 2024

GoAnywhere MFT Authentication Bypass

GoAnywhere MFT authentication bypass proof of concept exploit.

- Link

—

” “Tue, 23 Jan 2024

PRTG Authenticated Remote Code Execution

This Metasploit module exploits an authenticated remote code execution vulnerability in PRTG.

- Link

—

” “Tue, 23 Jan 2024

Solar FTP Server 2.1.2 Denial Of Service

Solar FTP Server version 2.1.2 remote denial of service exploit.

- Link

—

” “Mon, 22 Jan 2024

MajorDoMo Command Injection

This Metasploit module exploits a command injection vulnerability in MajorDoMo versions before 0662e5e.

- Link

—

” “Mon, 22 Jan 2024

Ivanti Connect Secure Unauthenticated Remote Code Execution

This Metasploit module chains an authentication bypass vulnerability and a command injection vulnerability to exploit vulnerable instances of either Ivanti Connect Secure or Ivanti Policy Secure, to

achieve unauthenticated remote code execution. All currently supported versions 9.x and 22.x prior to the vendor mitigation are vulnerable. It is unknown if unsupported versions 8.x and below are also vulnerable.

- Link

—

” “Mon, 22 Jan 2024

EzServer 6.4.017 Denial Of Service

EzServer version 6.4.017 remote denial of service exploit.

- Link

—

” “Mon, 22 Jan 2024

xbtitFM 4.1.18 SQL Injection / Shell Upload / Traversal

xbtitFM versions 4.1.18 and below suffer from remote shell upload, remote SQL injection, and path traversal vulnerabilities.

- Link

—

” “Mon, 22 Jan 2024

Golden FTP Server 2.02b Denial Of Service

Golden FTP Server version 2.02b remote denial of service exploit.

- Link

—

” “Mon, 22 Jan 2024

Traceroute 2.1.2 Privilege Escalation

In Traceroute versions 2.0.12 through to 2.1.2, the wrapper scripts mishandle shell metacharacters, which can lead to privilege escalation if the wrapper scripts are executed via sudo. The affected wrapper scripts include tcptraceroute, tracepath, traceproto, and traceroute-nanog. Version 2.1.3 addresses this issue.

- Link

—

” “Mon, 22 Jan 2024

TrojanSpy Win32 Nivdort MVID-2024-0668 Insecure Permissions

TrojanSpy Win32 Nivdort malware suffers from an insecure permissions vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 “Wir sind SeCurItY HeRsTelLeR”... jaja, geh wieder schlafen

Zum Youtube Video

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-25	Group Health Cooperative of South Central Wisconsin	[USA]	Link
2024-01-25	Santa Cruz do Sul	[BRA]	Link
2024-01-24	Comté de Washington, Pennsylvanie	[USA]	Link
2024-01-24	Centre de coordination des services de communication en santé (CCSC)	[CAN]	Link
2024-01-24	The Misbourne School	[GBR]	Link
2024-01-23	Département de la Sarthe	[FRA]	Link
2024-01-23	Kansas City Area Transportation Authority (KCATA)	[USA]	Link
2024-01-22	EquiLend	[USA]	Link
2024-01-22	Volkshochschule (VHS) Minden-Bad Oeynhausen	[DEU]	Link
2024-01-22	ICN Business School Nancy	[FRA]	Link
2024-01-21	Bucks County	[USA]	Link
2024-01-20	Caravan and Motorhome Club (CAMC)	[GBR]	Link
2024-01-19	Town of Greater Napanee	[CAN]	Link
2024-01-19	Tietoevry	[SWE]	Link
2024-01-19	Clackamas Community College	[USA]	Link
2024-01-19	Japan Food Holdings	[SGP]	Link
2024-01-17	Donau 3 FM	[DEU]	Link
2024-01-17	Service de secours de Jämtland	[SWE]	Link
2024-01-17	V.I. Lottery (Loterie des Îles Vierges)	[VIR]	Link
2024-01-17	Veolia North America	[USA]	Link
2024-01-16	Université d'État du Kansas (K-State)	[USA]	Link
2024-01-15	Foxsemicon Integrated Technology Inc (□□□□)	[TWN]	Link

Datum	Opfer	Land	Information
2024-01-15	Canterbury City Council, Thanet District Council, Dover District Council.	[GBR]	Link
2024-01-14	Douglas County Libraries	[USA]	Link
2024-01-13	Calvia	[ESP]	Link
2024-01-13	Sambr'Habitat	[BEL]	Link
2024-01-10	RE&S Holdings	[JPN]	Link
2024-01-10	Lush	[GBR]	Link
2024-01-06	loanDepot	[USA]	Link
2024-01-06	Banque nationale d'Angola	[AGO]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-28	[mordfin]	qilin	Link
2024-01-27	[oogp.com]	cactus	Link
2024-01-27	[vidalung.ai]	abyss	Link
2024-01-26	[Kansas City Area Transportation Authority]	medusa	Link
2024-01-26	[Cislo & Thomas LLP]	bianlian	Link
2024-01-26	[Image Craft]	bianlian	Link
2024-01-26	[Shoma group]	bianlian	Link
2024-01-26	[ehsd.org]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-25	[US government (private data) +Rothschild&Rockefeller]	snatch	Link
2024-01-26	[sipicorp.com]	blackbasta	Link
2024-01-26	[Brazilian Business Park]	akira	Link
2024-01-26	[elandenergy.com Eland Energy]	mydata	Link
2024-01-26	[Valley TeleCom Group]	akira	Link
2024-01-26	[securinux.net]	lockbit3	Link
2024-01-26	[jaygroup.com]	cactus	Link
2024-01-26	[Draneas Huglin Dooley LLC]	alphv	Link
2024-01-25	[Lush]	akira	Link
2024-01-25	[OrthoNY, Orthopedic Care]	incransom	Link
2024-01-25	[Four Hands LLC]	0mega	Link
2024-01-25	[CloudFire Italy]	medusa	Link
2024-01-25	[leclairgroup.com]	blackbasta	Link
2024-01-25	[NOVA Business Law Group]	bianlian	Link
2024-01-25	[The Wiser Financial Group]	bianlian	Link
2024-01-25	[ANI Networks]	akira	Link
2024-01-25	[caravanclub.co.uk]	lockbit3	Link
2024-01-25	[Toronto Zoo]	akira	Link
2024-01-25	[wannagocloud]	qilin	Link
2024-01-25	[neafidi]	qilin	Link
2024-01-24	[Brightstar Care]	alphv	Link
2024-01-24	[Hawbaker Engineering]	ransomhouse	Link
2024-01-24	[Charles Trent]	hunters	Link
2024-01-24	[Innovative Automation]	hunters	Link
2024-01-24	[Tamdown]	hunters	Link
2024-01-24	[Thorite Group]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-23	[US government (private data)]	snatch	Link
2024-01-24	[icn-artem.com]	lockbit3	Link
2024-01-24	[SANDALAWOFFICES.COM]	clop	Link
2024-01-24	[IntegrityInc.org Integrity Inc]	mydata	Link
2024-01-24	[https://www.carri.com]	mydata	Link
2024-01-24	[https://www.gadotbio.com/ Gadot Biochemical Industries Ltd]	mydata	Link
2024-01-24	[accolade-group.com + levelwear.com +Taiwan microelectronics(CRM).]	mydata	Link
2024-01-24	[a24group.com ambition24hours.co.za]	mydata	Link
2024-01-24	[https://www.mikeferry.com]	mydata	Link
2024-01-24	[Dirig Sheet Metal]	akira	Link
2024-01-24	[Winona Pattern & Mold]	meow	Link
2024-01-24	[Signature Performance Insurance]	medusa	Link
2024-01-24	[MBC Law Professional Corporation]	alphv	Link
2024-01-24	[Groupe Sweetco]	8base	Link
2024-01-24	[Bikesportz Imports]	8base	Link
2024-01-24	[La Ligue]	8base	Link
2024-01-24	[Midwest Service Center]	8base	Link
2024-01-24	[Sunfab Hydraulics AB]	8base	Link
2024-01-24	[Glimstedt]	8base	Link
2024-01-19	[FULL LEAK! Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-23	[synergyfinancialgrp.com]	abyss	Link
2024-01-23	[micrometals.com]	abyss	Link
2024-01-23	[lyonshipyard.com]	lockbit3	Link
2024-01-23	[sierrafrontgroup.com]	lockbit3	Link
2024-01-23	[Cryopak]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-23	[fairmontfcu.com]	blackbasta	Link
2024-01-23	[ktbslaw.com]	blackbasta	Link
2024-01-23	[dupont-restauration.fr]	blackbasta	Link
2024-01-23	[kivibros.com]	blackbasta	Link
2024-01-23	[haes.ca]	blackbasta	Link
2024-01-23	[cinfab.com]	blackbasta	Link
2024-01-23	[prudentpublishing.com]	blackbasta	Link
2024-01-23	[unitedindustries.co.nz]	blackbasta	Link
2024-01-23	[stemcor.com]	blackbasta	Link
2024-01-23	[Wilhoit Properties]	akira	Link
2024-01-23	[Milestone Environmental Contracting]	akira	Link
2024-01-23	[Total Air Solutions]	alphv	Link
2024-01-22	[Double Eagle Energy Holdings IV]	hunters	Link
2024-01-23	[R.C. Moore Trucking]	hunters	Link
2024-01-23	[envea.global]	blackbasta	Link
2024-01-23	[Herrs (You have 72 hours)]	alphv	Link
2024-01-21	[Smith Capital - Press Release]	monti	Link
2024-01-16	[ARPEGE]	8base	Link
2024-01-09	[C and F Packing Company Inc.]	8base	Link
2024-01-22	[HOE Pharmaceuticals Sdn Bhd]	ransomhouse	Link
2024-01-22	[davidsbridal.com]	lockbit3	Link
2024-01-22	[agc.com]	blackbasta	Link
2024-01-22	[Double Eagle Development]	hunters	Link
2024-01-22	[southernwater.co.uk]	blackbasta	Link
2024-01-22	[Waldner’s]	medusa	Link
2024-01-22	[Pozzi Italy]	medusa	Link
2024-01-22	[The Gainsborough Bath]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-22	[Richmond Fellowship Scotland]	medusa	Link
2024-01-22	[ANS COMPUTER [72hrs]]	alphv	Link
2024-01-18	[deknudtframes.be]	cuba	Link
2024-01-21	[synnex-grp.com]	lockbit3	Link
2024-01-21	[gattoplaters.com]	lockbit3	Link
2024-01-21	[duconind.com]	lockbit3	Link
2024-01-21	[wittmann.at]	lockbit3	Link
2024-01-21	[qtc-energy.com]	lockbit3	Link
2024-01-21	[hughessupplyco.com]	lockbit3	Link
2024-01-21	[umi-tiles.com]	lockbit3	Link
2024-01-21	[cct.or.th]	lockbit3	Link
2024-01-22	[cmmt.com.tw]	lockbit3	Link
2024-01-21	[shenandoahtx.us]	lockbit3	Link
2024-01-21	[stjohnrochester.org]	lockbit3	Link
2024-01-21	[bmc-cpa.com]	lockbit3	Link
2024-01-21	[jasman.com.mx]	lockbit3	Link
2024-01-21	[North Star Tax And Accounting]	bianlian	Link
2024-01-21	[KC Pharmaceuticals]	bianlian	Link
2024-01-21	[Martinaire Aviation]	bianlian	Link
2024-01-21	[subway.com]	lockbit3	Link
2024-01-21	[tvjahnrheine.de]	lockbit3	Link
2024-01-21	[marxan.es]	lockbit3	Link
2024-01-21	[home-waremmien.be]	lockbit3	Link
2024-01-20	[wendy.mx]	lockbit3	Link
2024-01-20	[swiftair.com]	lockbit3	Link
2024-01-20	[Worthen Industries [You have three days]]	alphv	Link
2024-01-19	[Anna Jaques Hospital]	moneymessage	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-19	[pratt.edu]	lockbit3	Link
2024-01-19	[seiu1000.org]	lockbit3	Link
2024-01-19	[Sykes Consulting, Inc.]	incransom	Link
2024-01-19	[dywidag.com]	lockbit3	Link
2024-01-19	[TPG Architecture]	play	Link
2024-01-12	[jdbchina.com]	lockbit3	Link
2024-01-19	[Hamilton-Madison House]	akira	Link
2024-01-19	[Hydratek]	akira	Link
2024-01-19	[Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-19	[evit.edu]	lockbit3	Link
2024-01-19	[Alupar Investimento SA]	hunters	Link
2024-01-19	[PROJECTSW]	qilin	Link
2024-01-19	[foxsemicon.com]	lockbit3	Link
2024-01-09	[Malongo France]	8base	Link
2024-01-18	[Samuel Sekuritas Indonesia & Samuel Aset Manajemen]	trigona	Link
2024-01-18	[Premier Facility Management]	trigona	Link
2024-01-18	[Fertility North]	trigona	Link
2024-01-18	[Vision Plast]	trigona	Link
2024-01-18	[uffs.edu.br]	stormous	Link
2024-01-18	[Groveport Madison Schools]	blacksuit	Link
2024-01-18	[GROWTH by NCRC]	bianlian	Link
2024-01-18	[LT Business Dynamics]	bianlian	Link
2024-01-18	[digipwr.com]	lockbit3	Link
2024-01-18	[jaffeandasher.com]	lockbit3	Link
2024-01-18	[Gallup McKinley County Schools]	hunters	Link
2024-01-15	[aercap.com]	slug	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-17	[DENHAM the Jeanmaker]	akira	Link
2024-01-17	[Stone, Avant & Daniels]	medusa	Link
2024-01-17	[JspPharma]	insane	Link
2024-01-16	[Axfast AB]	8base	Link
2024-01-16	[Syndicat Général des Vignerons de la Champagne]	8base	Link
2024-01-16	[Washtech]	8base	Link
2024-01-16	[SIVAM Coatings S.p.A.]	8base	Link
2024-01-16	[Nexus Telecom Switzerland AG]	8base	Link
2024-01-16	[millgate.co.uk]	lockbit3	Link
2024-01-16	[Becker Logistics]	akira	Link
2024-01-16	[Bestway Sales]	akira	Link
2024-01-16	[TGS Transportation]	akira	Link
2024-01-16	[Premium Guard]	akira	Link
2024-01-16	[F J O’Hara & Sons]	qilin	Link
2024-01-16	[Donear Industries]	bianlian	Link
2024-01-15	[Beit Handesai]	malekteam	Link
2024-01-15	[shinwajpn.co.jp]	lockbit3	Link
2024-01-15	[maisonsdelavenir.com]	lockbit3	Link
2024-01-15	[vasudhapharma.com]	lockbit3	Link
2024-01-15	[hosted-it.co.uk]	lockbit3	Link
2024-01-15	[Ausa]	hunters	Link
2024-01-15	[Republic Shipping Consolidators, Inc]	bianlian	Link
2024-01-15	[Northeast Spine and Sports Medicine’s]	bianlian	Link
2024-01-14	[SPARTAN Light Metal Products]	unsafe	Link
2024-01-14	[Hartl European Transport Company]	unsafe	Link
2024-01-14	[American International College]	unsafe	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-14	[www.kai.id “FF”]	stormous	Link
2024-01-14	[amenitek.com]	lockbit3	Link
2024-01-08	[turascandinavia.com]	lockbit3	Link
2024-01-13	[Lee Spring]	rhysida	Link
2024-01-11	[Charm Sciences]	snatch	Link
2024-01-11	[Malabar Gold & Diamonds]	snatch	Link
2024-01-11	[Banco Promerica]	snatch	Link
2024-01-12	[arrowinternational.com]	lockbit3	Link
2024-01-12	[thecsi.com]	threeam	Link
2024-01-12	[pharrusa.com]	threeam	Link
2024-01-12	[Builcore]	alphv	Link
2024-01-12	[hotelcontinental.no]	qilin	Link
2024-01-12	[olea.com]	lockbit3	Link
2024-01-12	[asburyauto.com]	cactus	Link
2024-01-12	[Washington School For The Deaf]	incransom	Link
2024-01-12	[Former S.p.A.]	8base	Link
2024-01-12	[International Trade Brokers and Forwarders]	8base	Link
2024-01-12	[BALLAY MENUISERIES]	8base	Link
2024-01-12	[Anderson King Energy Consultants, LLC]	8base	Link
2024-01-12	[Sems and Specials Incorporated]	8base	Link
2024-01-12	[acutis.com]	cactus	Link
2024-01-12	[dtsolutions.net]	cactus	Link
2024-01-12	[intercityinvestments.com]	cactus	Link
2024-01-12	[hi-cone.com]	cactus	Link
2024-01-12	[Alliedwoundcare]	everest	Link
2024-01-12	[Primeimaging]	everest	Link
2024-01-11	[Blackburn College]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-11	[Vincentz Network]	akira	Link
2024-01-11	[Limburg]	medusa	Link
2024-01-11	[Water For People]	medusa	Link
2024-01-11	[pactchangeslives.com]	lockbit3	Link
2024-01-11	[Triella]	alphv	Link
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	Link
2024-01-11	[SHIBLEY RIGHTON]	alphv	Link
2024-01-11	[automotionshade.com]	alphv	Link
2024-01-11	[R Robertson Insurance Brokers]	alphv	Link
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twt.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	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.