Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240226

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

WS_FTP: Updates dichten hochriskante Sicherheitslücke ab

In WS-FTP von Progress klafft eine Sicherheitslücke, die Angreifern Cross-Site-Scripting-Angriffe ermöglicht. Ein Update steht bereit.

- Link

—

Sicherheitslücken: GitLab gegen mögliche Attacken abgesichert

Updates schließen mehrere Schwachstellen in GitLab. Eine Lücke bleibt aber offensichtlich erstmal bestehen.

- Link

—

Sicherheitsupdate: Root-Lücke bedroht Servermonitoringtool Nagios XI

Admins sollten das Dienste-Monitoring mit Nagios XI aus Sicherheitsgründen zeitnah auf den aktuellen Stand bringen.

- Link

—

CMS Joomla bessert riskante Schwachstellen aus

Das Joomla-Projekt schließt mit den Versionen 5.0.3 und 4.4.3 Sicherheitslücken. Angreifer können dadurch etwa Dateien manipulieren.

- Link

—

HP Laser-Drucker: Sicherheitslücken erlauben Codeschmuggel

HP warnt mit gleich zwei Sicherheitsmeldungen vor Lücken in diversen Laserjet-Druckern. Firmwareupdates sollen sie schließen.

- Link

—

Broadcom schließt Sicherheitslücken in VMware Aria Operations und EAP-Plug-in

Broadcom verteilt Updates für VMware Aria Operations und das EAP Browser Plug-in. Sie bessern teils kritische Sicherheitslücken aus.

- Link

—

Firefox und Thunderbird: Neue Versionen liefern Sicherheitsfixes

Neue Versionen von Firefox, Firefox ESR und Thunderbird stehen bereit. Sie dichten im Kern Sicherheitslücken ab.

- Link

—

Google Chrome 122: Zwölf Sicherheitslecks gestopft

Der Versionszweig 122 von Google Chrome bessert vor allem zwölf Schwachstellen aus.

- Link

—

Jetzt updaten: Kritische Codeschmuggel-Lücken in Connectwise Screenconnect

In der Remote-Desktop-Software Screenconnect von Connectwise klaffen teils kritische Sicherheitslücken. Sie erlauben das Einschleusen von Schadcode.

- Link

—

Solarwinds: Codeschmuggel möglich, Updates verfügbar

Solarwinds schließt Sicherheitslücken in Access Rights Manager und Platform (Orion). Angreifer können Schadcode einschleusen.

- 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	0.916210000	0.988200000	Link
CVE-2023-5360	0.967230000	0.996310000	Link
CVE-2023-4966	0.963970000	0.995200000	Link
CVE-2023-47246	0.943540000	0.991300000	Link
CVE-2023-46805	0.962740000	0.994830000	Link
CVE-2023-46747	0.971390000	0.997740000	Link
CVE-2023-46604	0.972850000	0.998430000	Link
CVE-2023-43177	0.932620000	0.990010000	Link
CVE-2023-42793	0.972940000	0.998500000	Link
CVE-2023-41265	0.915100000	0.988060000	Link
CVE-2023-39143	0.925430000	0.989200000	Link
CVE-2023-38646	0.903940000	0.987150000	Link
CVE-2023-38205	0.934710000	0.990180000	Link
CVE-2023-38035	0.974110000	0.999230000	Link
CVE-2023-36845	0.965590000	0.995780000	Link
CVE-2023-3519	0.908750000	0.987570000	Link
CVE-2023-35082	0.962890000	0.994890000	Link
CVE-2023-35078	0.949930000	0.992270000	Link
CVE-2023-34960	0.925010000	0.989180000	Link
CVE-2023-34634	0.919000000	0.988490000	Link
CVE-2023-34362	0.959040000	0.993970000	Link
CVE-2023-3368	0.928930000	0.989540000	Link
CVE-2023-33246	0.973410000	0.998770000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32315	0.973860000	0.999040000	Link
CVE-2023-32235	0.902020000	0.987060000	Link
CVE-2023-30625	0.951530000	0.992540000	Link
CVE-2023-30013	0.936180000	0.990340000	Link
CVE-2023-29300	0.959640000	0.994120000	Link
CVE-2023-28771	0.923800000	0.989040000	Link
CVE-2023-28121	0.933120000	0.990060000	Link
CVE-2023-27524	0.972330000	0.998210000	Link
CVE-2023-27372	0.971580000	0.997800000	Link
CVE-2023-27350	0.972270000	0.998180000	Link
CVE-2023-26469	0.946560000	0.991750000	Link
CVE-2023-26360	0.960730000	0.994390000	Link
CVE-2023-26035	0.969370000	0.996950000	Link
CVE-2023-25717	0.962180000	0.994680000	Link
CVE-2023-2479	0.964780000	0.995420000	Link
CVE-2023-24489	0.973500000	0.998840000	Link
CVE-2023-23752	0.948570000	0.992110000	Link
CVE-2023-23397	0.917330000	0.988310000	Link
CVE-2023-22527	0.965680000	0.995810000	Link
CVE-2023-22518	0.969180000	0.996890000	Link
CVE-2023-22515	0.973330000	0.998730000	Link
CVE-2023-21839	0.962110000	0.994660000	Link
CVE-2023-21554	0.961220000	0.994460000	Link
CVE-2023-20887	0.965640000	0.995790000	Link
CVE-2023-20198	0.919220000	0.988510000	Link
CVE-2023-1671	0.964250000	0.995290000	Link
CVE-2023-0669	0.968020000	0.996560000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 23 Feb 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] Apple iOS und Apple iPadOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 23 Feb 2024

[NEU] [hoch] VMware Enhanced Authentication Plug-in (EAP): Mehrere Schwachstellen ermöglichen die Umgehung von Sicherheitsmaßnahmen und die Ausweitung von Berechtigungen

Ein Angreifer kann mehrere Schwachstellen im VMware Enhanced Authentication Plug-in (EAP) ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder seine Berechtigungen zu erweitern.

- Link

—

Fri, 23 Feb 2024

[NEU] [hoch] Mozilla Firefox: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 23 Feb 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Kemp LoadMaster ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] ImageMagick: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ImageMagick ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

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

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Fri, 23 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [hoch] HP LaserJet: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in HP LaserJet ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 23 Feb 2024

[UPDATE] [kritisch] ConnectWise ScreenConnect: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in ConnectWise ScreenConnect ausnutzen, um Informationen offenzulegen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 22 Feb 2024

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, Dateien zu manipulieren, seine Privilegien zu erweitern oder einen Cross-Site-Scripting (XSS)-Angriff durchzuführen.

- Link

—

Thu, 22 Feb 2024

[NEU] [hoch] Nagios Enterprises Nagios XI: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Nagios Enterprises Nagios XI ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen Cross-Site-Scripting (XSS)-Angriff durchzuführen.

- Link

—

Thu, 22 Feb 2024

[NEU] [UNGEPATCHT] [kritisch] D-LINK Router: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 22 Feb 2024

[NEU] [UNGEPATCHT] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

—

Thu, 22 Feb 2024

[NEU] [hoch] Liferay Portal und DXP: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Liferay Liferay DXP und Liferay Liferay Portal ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.
- Link

—

Thu, 22 Feb 2024

[UPDATE] [hoch] Cisco Adaptive Security Appliance (ASA) und Cisco Firepower Threat Defense (FTD): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco Adaptive Security Appliance (ASA) und Cisco Firepower Threat Defense (FTD) ausnutzen, um einen Denial of Service Angriff durchzuführen, Daten zu manipulieren oder vertrauliche Informationen einzusehen.
- Link

—

Thu, 22 Feb 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/25/2024	[Fedora 38 : mingw-openexr (2024-f4d51715fe)]	critical
2/25/2024	[Fedora 39 : mingw-openexr (2024-7fc5bae919)]	critical
2/25/2024	[Debian dsa-5631 : iwd - security update]	critical

Datum	Schwachstelle	Bewertung
2/24/2024	[Fedora 39 : mingw-qt5-qt3d / mingw-qt5-qtactiveqt / mingw-qt5-qtbase / etc (2024-a8cdce27ac)]	critical
2/23/2024	[SUSE SLES15 / openSUSE 15 Security Update : python-uamqp (SUSE-SU-2024:0591-1)]	critical
2/23/2024	[SUSE SLES12 Security Update : docker (SUSE-SU-2024:0587-1)]	critical
2/23/2024	[Liferay Portal 7.4.x < 7.4.3.102 XSS]	critical
2/23/2024	[Liferay Portal 7.4.x < 7.4.3.4 Multiple Vulnerabilities]	critical
2/23/2024	[Liferay Portal 7.4.x < 7.4.3.14 XSS]	critical
2/23/2024	[Liferay Portal 7.4.x < 7.4.3.98 Multiple Vulnerabilities]	critical
2/23/2024	[Liferay Portal 7.4.x < 7.4.3.5 XSS]	critical
2/23/2024	[SonicWall SonicOS Buffer Overflow (SNWLID-2022-0003)]	critical
2/23/2024	[FreeBSD : suricata – multiple vulnerabilities (979dc373-d27d-11ee-8b84-b42e991fc52e)]	critical
2/23/2024	[FreeBSD : electron27 – multiple vulnerabilities (80ad6d6c-b398-457f-b88f-bf6be0bbad44)]	critical
2/25/2024	[Fedora 38 : dhcpcd (2024-2bb2bb2467)]	high
2/25/2024	[Fedora 38 : chromium (2024-6a879cfa63)]	high
2/25/2024	[Fedora 39 : mingw-expat (2024-fbe1f0c1aa)]	high
2/25/2024	[Fedora 38 : mingw-expat (2024-b8656bc059)]	high
2/25/2024	[FreeBSD : gitea – Fix XSS vulnerabilities (5ecfb588-d2f4-11ee-ad82-dbdfaa8acfc2)]	high
2/25/2024	[CentOS 8 : unbound (CESA-2024:0965)]	high
2/24/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2024:0607-1)]	high
2/24/2024	[SUSE SLES15 Security Update : qemu (SUSE-SU-2024:0589-1)]	high
2/24/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:0608-1)]	high

Datum	Schwachstelle	Bewertung
2/24/2024	[Amazon Linux AMI : sudo (ALAS-2024-1922)]	high
2/24/2024	[Amazon Linux 2 : sudo (ALAS-2024-2473)]	high
2/24/2024	[Oracle Linux 9 : firefox (ELSA-2024-0952)]	high
2/24/2024	[Fedora 38 : expat (2024-8a2c093df5)]	high
2/24/2024	[SUSE SLES12 Security Update : java-1_8_0-ibm (SUSE-SU-2024:0605-1)]	high
2/24/2024	[FreeBSD : chromium – multiple security fixes (2a470712-d351-11ee-86bb-a8a1599412c6)]	high
2/23/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : tiff (SUSE-SU-2024:0594-1)]	high
2/23/2024	[SUSE SLES15 / openSUSE 15 Security Update : php-composer2 (SUSE-SU-2024:0592-1)]	high
2/23/2024	[Oracle Linux 8 : go-toolset:ol8 (ELSA-2024-0887)]	high
2/23/2024	[Debian dsa-5629 : chromium - security update]	high
2/23/2024	[RHEL 8 : kpatch-patch (RHSA-2024:0937)]	high
2/23/2024	[Debian dsa-5630 : thunderbird - security update]	high
2/23/2024	[Oracle Linux 9 : postgresql (ELSA-2024-0951)]	high
2/23/2024	[Ubuntu 23.10 : Linux kernel (Azure) vulnerabilities (USN-6652-1)]	high
2/23/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6651-1)]	high
2/23/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6653-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Sat, 24 Feb 2024

Tosibox Key Service 3.3.0 Local Privilege Escalation / Unquoted Service Path

Tosibox Key Service versions 3.3.0 and below suffer from an unquoted search path issue impacting the service Tosibox Key Service for Windows. This could potentially allow an authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system.

- Link

—

” “Sat, 24 Feb 2024

Backdoor.Win32.Armageddon.r MVID-2024-0670 Hardcoded Credential

Backdoor.Win32.Armageddon.r malware suffers from a hardcoded credential vulnerability.

- Link

—

” “Sat, 24 Feb 2024

ConnectWise ScreenConnect 23.9.7 Unauthenticated Remote Code Execution

This Metasploit module exploits an authentication bypass vulnerability that allows an unauthenticated attacker to create a new administrator user account on a vulnerable ConnectWise ScreenConnect server. The attacker can leverage this to achieve remote code execution by uploading a malicious extension module. All versions of ScreenConnect version 23.9.7 and below are affected.

- Link

—

” “Sat, 24 Feb 2024

SuperCali 1.1.0 Cross Site Scripting

SuperCali version 1.1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 22 Feb 2024

QNAP QTS / QuTS Hero Unauthenticated Remote Code Execution

There exists an unauthenticated command injection vulnerability in the QNAP operating system known as QTS and QuTS hero. QTS is a core part of the firmware for numerous QNAP entry and mid-level Network Attached Storage (NAS) devices, and QuTS hero is a core part of the firmware for numerous QNAP high-end and enterprise NAS devices. The vulnerable endpoint is the quick.cgi component, exposed by the device’s web based administration feature. The quick.cgi component is present in an uninitialized QNAP NAS device. This component is intended to be used during either manual or cloud based provisioning of a QNAP NAS device. Once a device has been successfully initialized, the quick.cgi component is disabled on the system. An attacker with network access to an uninitialized QNAP NAS device may perform unauthenticated command injection, allowing the attacker to execute arbitrary commands on the device.

- Link

—

” “Thu, 22 Feb 2024

CMS Made Simple 2.2.19 Server-Side Template Injection

CMS Made Simple version 2.2.19 suffers from a server-side template injection vulnerability.

- Link

—

” “Thu, 22 Feb 2024

CMS Made Simple 2.2.19 Cross Site Scripting

CMS Made Simple version 2.2.19 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 22 Feb 2024

CMS Made Simple 2.2.19 Remote Code Execution

CMS Made Simple version 2.2.19 suffers from a remote code execution vulnerability.

- Link

—

” “Thu, 22 Feb 2024

SitePad 1.8.2 Cross Site Scripting

SitePad version 1.8.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 22 Feb 2024

Dotclear 2.29 Cross Site Scripting

Dotclear version 2.29 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 22 Feb 2024

FreeIPA 4.10.1 Denial Of Service / Information Disclosure

FreeIPA version 4.10.1 has an issue where specially crafted HTTP requests potentially lead to denial of service or data exposure.

- Link

—

” “Wed, 21 Feb 2024

OpenOLAT 18.1.5 Cross Site Scripting / Privilege Escalation

OpenOLAT versions 18.1.4 and below and versions 18.1.5 and below suffer from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Wed, 21 Feb 2024

Yealink Configuration Encrypt Tool Static AES Key

A single, vendorwide, hardcoded AES key in the Yealink Configuration Encrypt Tool used to encrypt provisioning documents was leaked leading to a compromise of confidentiality of provisioning documents.

- Link

—

” “Wed, 21 Feb 2024

Ivanti Connect Secure Unauthenticated Remote Code Execution

This Metasploit module chains a server side request forgery (SSRF) vulnerability (CVE-2024-21893) and a command injection vulnerability (CVE-2024-21887) 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 are vulnerable, prior to the vendor patch released on Feb 1, 2024. It is unknown if unsupported versions 8.x and below are also vulnerable.

- Link

—

” “Wed, 21 Feb 2024

WordPress 6.4.3 Username Disclosure

WordPress versions 6.4.3 and below appear to suffer from a REST API related username disclosure vulnerability.

- Link

—

” “Wed, 21 Feb 2024

Fuelflow 1.0 SQL Injection

Fuelflow version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 21 Feb 2024

ITFlow Cross Site Request Forgery

ITFlow versions prior to commit 432488eca3998c5be6b6b9e8f8ba01f54bc12378 suffer from a cross site request forgery vulnerability.

- Link

—

” “Wed, 21 Feb 2024

WEBIGniter 28.7.23 Cross Site Scripting

WEBIGniter version 28.7.23 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 20 Feb 2024

Kafka UI 0.7.1 Command Injection

A command injection vulnerability exists in Kafka UI versions 0.4.0 through 0.7.1 that allows an attacker to inject and execute arbitrary shell commands via the groovy filter parameter at the topic section.

- Link

—

” “Tue, 20 Feb 2024

Savsoft Quiz 6.0 Enterprise Cross Site Scripting

Savsoft Quiz version 6.0 Enterprise suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 20 Feb 2024

SPA-CART CMS 1.9.0.3 Cross Site Scripting

SPA-CART CMS version 1.9.0.3 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 20 Feb 2024

Petrol Pump Management Software 1.0 Shell Upload

Petrol Pump Management Software version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 20 Feb 2024

Tourism Management System 2.0 Shell Upload

Tourism Management System version 2.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Backdoor_JS.Relvelshe.A Detection / Mitigation Bypass

Back in 2022, the researcher released a proof of concept to bypass the Backdoor:JS/Relvelshe.A detection in Windows Defender but it no longer works as it was mitigated. However, adding a simple javascript try catch error statement and eval’ing the hex string, it executes as of the time of this post.

- Link

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Trojan.Win32/Powessere.G VBScript Detection Bypass

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass. This issue was addressed. The fix

was short lived as the researcher found yet another third trivial bypass. Previously, the researcher disclosed 3 bypasses using rundll32 javascript, but this example leverages the VBSCRIPT and ActiveX engines.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 23 Feb 2024
ZDI-24-205: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Fri, 23 Feb 2024
ZDI-24-204: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 23 Feb 2024
ZDI-24-203: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 23 Feb 2024
ZDI-24-202: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 23 Feb 2024
ZDI-24-201: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link
—
” “Fri, 23 Feb 2024
ZDI-24-200: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
- Link

—

” “Fri, 23 Feb 2024

ZDI-24-199: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-198: PDF-XChange Editor Updater Improper Certificate Validation Remote Code Execution Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-197: PDF-XChange Editor JPG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-196: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-195: Linux Kernel ksmbd TCP Connection Race Condition Remote Code Execution Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-194: Linux Kernel ksmbd Mech Token Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 23 Feb 2024

ZDI-24-193: Sante PACS Server Token Endpoint SQL Injection Remote Code Execution Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Zahnbürsten DDoS und bald hat Ivanti die OWASP Top 10 voll...

Zum Youtube Video

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-23	Gendarmerie royale du Canada (RCMP)	[CAN]	Link
2024-02-22	Verbraucherzentrale Hessen	[DEU]	Link
2024-02-22	Coocique	[CRI]	Link
2024-02-22	City of Oakley	[USA]	Link
2024-02-22	City of Pleasant Hill	[USA]	Link
2024-02-21	Service d'immigration du Malawi	[MWI]	Link
2024-02-20	Berliner Hochschule für Technik (BHT)	[DEU]	Link
2024-02-20	Continental Aerospace	[USA]	Link
2024-02-20	Change Healthcare	[USA]	Link
2024-02-19	Francis Howell School District	[USA]	Link
2024-02-18	Evangelische Landeskirche Hannovers	[DEU]	Link
2024-02-17	GCA (Charles André)	[FRA]	Link
2024-02-16	Government Employees Pension Fund (GEPF)	[ZAF]	Link
2024-02-15	PSI	[DEU]	Link
2024-02-15	Vili's Family Bakery	[AUS]	Link
2024-02-14	JCT600	[GBR]	Link
2024-02-13	Aztech Global	[SGP]	Link
2024-02-13	Varta	[DEU]	Link
2024-02-13	Coeur d'Alene	[USA]	Link
2024-02-13	Act21	[FRA]	Link
2024-02-13	School District 67	[CAN]	Link
2024-02-12	MSH International	[CAN]	Link
2024-02-11	Centre hospitalier d'Armentières	[FRA]	Link
2024-02-11	Hipocrate Information System (HIS)	[ROU]	Link

Datum	Opfer	Land	Information
2024-02-11	Clinique privée La Colline (groupe Hirslanden)	[CHE]	Link
2024-02-11	Consulting Radiologists Ltd.	[USA]	Link
2024-02-09	Office of Colorado State Public Defender	[USA]	Link
2024-02-07	Université de Central Missouri	[USA]	Link
2024-02-07	SouthState Bank	[USA]	Link
2024-02-07	Commune de Petersberg	[DEU]	Link
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	Link
2024-02-06	Commune de Kalmar	[SWE]	Link
2024-02-06	Advania	[SWE]	Link
2024-02-06	Onclusive	[GBR]	Link
2024-02-06	Kind	[DEU]	Link
2024-02-05	Prudential Financial, Inc.	[USA]	Link
2024-02-05	Central Arkansas Library System (CALS)	[USA]	Link
2024-02-04	Northern Light Health	[USA]	Link
2024-02-04	Middletown Area School District	[USA]	Link
2024-02-02	Germantown	[USA]	Link
2024-02-02	Université de Reykjavík	[ISL]	Link
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	Link
2024-02-02	Mairie de Korneuburg	[AUT]	Link
2024-02-02	Welch’s	[USA]	Link
2024-02-02	Etesia	[FRA]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	Link

Datum	Opfer	Land	Information
2024-02-01	Minnesota State University-Moorhead (MSUM)	[USA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-14	[Abelsantosyasoc]	stormous	Link
2024-02-14	[calcomp]	stormous	Link
2024-02-15	[bombaygrills]	stormous	Link
2024-02-25	[apeagers.com.au]	lockbit3	Link
2024-02-25	[Pot O’ Gold Coffee]	ciphbit	Link
2024-02-25	[AL SHEFA FARM]	ransomhub	Link
2024-02-25	[dunaway.com]	lockbit3	Link
2024-02-24	[crbgroup.com]	lockbit3	Link
2024-02-24	[nationaldentex.com]	lockbit3	Link
2024-02-24	[equilend.com]	lockbit3	Link
2024-02-24	[magierp.com]	lockbit3	Link
2024-02-24	[Spine West]	monti	Link
2024-02-24	[Roncelli Plastics]	bianlian	Link
2024-02-24	[Worthen Industries [FULL DATA]]	alphv	Link
2024-02-24	[GRUPOCREATIVO]	qilin	Link
2024-02-24	[kinematica.ch]	qilin	Link
2024-02-22	[Welch’s]	play	Link
2024-02-23	[IJM Corporation]	hunters	Link
2024-02-23	[Family Health center]	alphv	Link
2024-02-23	[remkes.nl]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-23	[APEX - apexspedition.de]	monti	Link
2024-02-23	[Acorn]	medusa	Link
2024-02-23	[Pressco Technology]	medusa	Link
2024-02-23	[ANDFLA SRL]	alphv	Link
2024-02-14	[C and J Industries, Inc.]	8base	Link
2024-02-22	[W???h?]	play	Link
2024-02-22	[team.jobs]	blackbasta	Link
2024-02-22	[Quik Pawn Shop]	akira	Link
2024-02-22	[PEER Consultants]	akira	Link
2024-02-22	[mtmrobotics.com]	threeam	Link
2024-02-22	[abcor.com.au]	threeam	Link
2024-02-22	[nfllp.com]	blackbasta	Link
2024-02-22	[climatech.com]	blackbasta	Link
2024-02-22	[usmerchants.com]	blackbasta	Link
2024-02-22	[birchallfoodservice.co.uk]	blackbasta	Link
2024-02-22	[dilweg.com]	blackbasta	Link
2024-02-22	[zircodata.com]	blackbasta	Link
2024-02-22	[Hardeman County Community Health Center]	alphv	Link
2024-02-22	[Worthen Industries [We’re giving you one last chance to save your business]]	alphv	Link
2024-02-21	[KHSS (You have 3 days)]	alphv	Link
2024-02-21	[Lancaster]	akira	Link
2024-02-21	[Desarrollo De Tecnologia y Sistemas Ltda]	akira	Link
2024-02-21	[HRTec Inc]	bianlian	Link
2024-02-21	[Marchassociates]	bianlian	Link
2024-02-21	[Austen Consultants]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-21	[dasteam.ch]	blackbasta	Link
2024-02-21	[doneff.com]	threeam	Link
2024-02-21	[Helical Technology]	8base	Link
2024-02-21	[Axel Johnson]	8base	Link
2024-02-20	[INFINITIUSA.COM]	mogilevich	Link
2024-02-20	[River Delta Unified School District]	meow	Link
2024-02-20	[Finlay Screening & Crushing Systems]	hunters	Link
2024-02-20	[Raocala]	everest	Link
2024-02-20	[advancedprosolutions.com]	cactus	Link
2024-02-19	[loransrl]	qilin	Link
2024-02-19	[soco.be]	lockbit3	Link
2024-02-19	[se.com]	cactus	Link
2024-02-19	[First Professional Services]	bianlian	Link
2024-02-19	[aivi.it]	trisec	Link
2024-02-19	[ki.se]	trisec	Link
2024-02-18	[Compression Leasing Services]	dragonforce	Link
2024-02-18	[Westward 360]	dragonforce	Link
2024-02-08	[aeromechinc.com]	lockbit3	Link
2024-02-18	[carlfischer.com]	lockbit3	Link
2024-02-17	[Bimbo Bakeries]	medusa	Link
2024-02-07	[bucher-strauss.ch]	lockbit3	Link
2024-02-16	[delia.pl]	stormous	Link
2024-02-14	[bombaygrills.com]	stormous	Link
2024-02-14	[calcomp.co.th]	stormous	Link
2024-02-02	[Abelsantosyasoc.com.ar]	stormous	Link
2024-02-18	[VSP Dental]	alphv	Link
2024-02-17	[Greater Napanee]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-17	[Tiete Automobile]	hunters	Link
2024-02-17	[Voice Technologies]	hunters	Link
2024-02-17	[Aftrp]	hunters	Link
2024-02-17	[Chicago Zoological Society]	hunters	Link
2024-02-17	[BS&B Safety Systems L.L.C]	hunters	Link
2024-02-17	[Wapiti Energy]	hunters	Link
2024-02-17	[PSI]	hunters	Link
2024-02-17	[CP Communications]	hunters	Link
2024-02-16	[Prudential Financial]	alphv	Link
2024-02-16	[LoanDepot]	alphv	Link
2024-02-16	[www.cogans.ie]	trisec	Link
2024-02-16	[The Chas. E. Phipps]	medusa	Link
2024-02-16	[BRONSTEIN-CARMONA.COM]	clop	Link
2024-02-14	[davidsbridal.com]	werewolves	Link
2024-02-16	[Réseau Ribé]	hunters	Link
2024-02-16	[BRAM Auto Group]	akira	Link
2024-02-16	[etisalat.ae]	lockbit3	Link
2024-02-16	[theclosingagent.com]	lockbit3	Link
2024-02-16	[spaldingssd.com]	lockbit3	Link
2024-02-16	[tormetal.cl]	lockbit3	Link
2024-02-16	[Concello de Teo]	hunters	Link
2024-02-16	[pacifica.co.uk]	blackbasta	Link
2024-02-16	[Ribe-Groupe]	hunters	Link
2024-02-16	[Griffin Dewatering]	hunters	Link
2024-02-15	[Dobrowski Stafford & Pierce]	bianlian	Link
2024-02-15	[LD Davis]	play	Link
2024-02-15	[von Hagen]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-15	[Norman, Fox]	play	Link
2024-02-15	[HR Ewell & Hy-tec]	play	Link
2024-02-15	[Mechanical Reps]	play	Link
2024-02-15	[Onclusive]	play	Link
2024-02-15	[MeerServices]	play	Link
2024-02-15	[DuBose Strapping]	play	Link
2024-02-15	[SilverLining]	play	Link
2024-02-15	[Schuster Trucking Company]	hunters	Link
2024-02-15	[Asam]	akira	Link
2024-02-15	[Advantage Orthopedic & Sports Medicine Clinic]	bianlian	Link
2024-02-12	[Rush Energy Services Inc [Time's up]]	alphv	Link
2024-02-13	[Hawbaker Engineering]	snatch	Link
2024-02-15	[ASP BasilicataASM MateraIRCCS CROB]	rhysida	Link
2024-02-15	[champion.com.co]	lockbit3	Link
2024-02-15	[coreengg.com]	lockbit3	Link
2024-02-15	[sitrack.com]	lockbit3	Link
2024-02-15	[hatsinteriors.com]	lockbit3	Link
2024-02-15	[pradiergranulats.fr]	lockbit3	Link
2024-02-15	[centralepaysanne.lu]	lockbit3	Link
2024-02-15	[ASA Electronics [2.7 TB]]	alphv	Link
2024-02-14	[studiogalbusera.com]	lockbit3	Link
2024-02-14	[Nekoosa School District]	akira	Link
2024-02-14	[BM Catalysts bmcatalysts.co.uk]	alphalocker	Link
2024-02-14	[vanwingerden.com]	abyss	Link
2024-02-14	[KALEEDS]	qilin	Link
2024-02-14	[conseguros]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-14	[kabat.pl]	lockbit3	Link
2024-02-13	[Sindicato de Enfermería (SATSE)]	hunters	Link
2024-02-13	[wsnelson.com]	lockbit3	Link
2024-02-13	[fultoncountyga.gov]	lockbit3	Link
2024-02-14	[UNIFER]	8base	Link
2024-02-14	[Institutional Casework, Inc]	8base	Link
2024-02-14	[ATB SA Ingénieurs-conseils SIA]	8base	Link
2024-02-14	[mmiculinary.com]	lockbit3	Link
2024-02-12	[adioscancer.com]	lockbit3	Link
2024-02-14	[giraud]	qilin	Link
2024-02-13	[rajawali.com]	lockbit3	Link
2024-02-13	[motilaloswal.com]	lockbit3	Link
2024-02-13	[barberemerson.com]	blackbasta	Link
2024-02-13	[ffppkg.co.uk]	blackbasta	Link
2024-02-13	[patriziapepe.com]	blackbasta	Link
2024-02-13	[btl.info]	blackbasta	Link
2024-02-13	[globalrescue.com]	blackbasta	Link
2024-02-13	[ssmnlaw.com]	blackbasta	Link
2024-02-13	[leonardssyrups.com]	blackbasta	Link
2024-02-13	[ROOSENS BÉTONS]	qilin	Link
2024-02-13	[universalservicesms.com]	lockbit3	Link
2024-02-13	[Communication Federal Credit Union]	hunters	Link
2024-02-13	[doprastav.sk]	lockbit3	Link
2024-02-13	[The Source]	alphv	Link
2024-02-13	[ArcisGolf]	alphv	Link
2024-02-13	[Trans-Northern Pipelines]	alphv	Link
2024-02-13	[Herrs]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-13	[Procopio]	alphv	Link
2024-02-13	[New Indy Containerboard]	alphv	Link
2024-02-13	[auruminstitute.org]	lockbit3	Link
2024-02-10	[SOPEM]	hunters	Link
2024-02-13	[Satse]	hunters	Link
2024-02-13	[Sanok Rubber CompanySpólka Akcyjna]	akira	Link
2024-02-12	[garonproducts.com]	threeam	Link
2024-02-07	[tecasrl.it]	lockbit3	Link
2024-02-12	[Antunovich Associates]	blacksuit	Link
2024-02-12	[DHX–Dependable Hawaiian Express]	knight	Link
2024-02-12	[Forgepresion.com]	cloak	Link
2024-02-12	[Rush Energy Services Inc [You have 48 hours]]	alphv	Link
2024-02-12	[SERCIDE]	alphv	Link
2024-02-12	[Lower Valley Energy, Inc]	alphv	Link
2024-02-12	[Modern Kitchens]	medusa	Link
2024-02-12	[vhprimary.com]	lockbit3	Link
2024-02-12	[germaintoiture.fr]	lockbit3	Link
2024-02-12	[Disaronno International]	meow	Link
2024-02-12	[Allmetal Inc.]	meow	Link
2024-02-12	[Freedom Munitions]	meow	Link
2024-02-12	[Arlington Perinatal Associates]	meow	Link
2024-02-12	[jacksonvillebeach.org]	lockbit3	Link
2024-02-12	[robs.org]	lockbit3	Link
2024-02-12	[parkhomeassist.co.uk]	lockbit3	Link
2024-02-12	[grotonschools.org]	lockbit3	Link
2024-02-12	[isspol.gov]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-12	[lyon.co.uk]	lockbit3	Link
2024-02-12	[dienerprecisionpumps.com]	lockbit3	Link
2024-02-12	[envie.org]	lockbit3	Link
2024-02-12	[sealco-leb.com]	lockbit3	Link
2024-02-12	[camarotto.it]	lockbit3	Link
2024-02-12	[paltertonprimary.co.uk]	lockbit3	Link
2024-02-12	[fidcornelis.be]	lockbit3	Link
2024-02-12	[plexustelerad.com]	lockbit3	Link
2024-02-12	[cabc.com.ar]	lockbit3	Link
2024-02-12	[textiles.org.tw]	lockbit3	Link
2024-02-12	[silverairways.com]	lockbit3	Link
2024-02-12	[Kreyenhop & Kluge]	hunters	Link
2024-02-12	[Kadac Australia]	medusa	Link
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	Link
2024-02-11	[lacolline-skincare.com]	lockbit3	Link
2024-02-10	[Upper Merion Township]	qilin	Link
2024-02-10	[YKP LTDA]	ransomhub	Link
2024-02-10	[Village of Skokie]	hunters	Link
2024-02-10	[Lancaster County Sheriff’s Office]	hunters	Link
2024-02-10	[Nastech]	hunters	Link
2024-02-10	[Benchmark Management Group]	hunters	Link
2024-02-10	[SOPEM Tunisie]	hunters	Link
2024-02-10	[Impact Energy Services]	hunters	Link
2024-02-10	[Groupe Goyette]	hunters	Link
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	Link
2024-02-10	[Carespring Health Care]	hunters	Link
2024-02-10	[Avianor Aircraft]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-10	[mranet.org]	abyss	Link
2024-02-10	[aisg-online.com]	lockbit3	Link
2024-02-10	[maddockhenson]	alphv	Link
2024-02-10	[verdimed.es]	lockbit3	Link
2024-02-10	[Pacific American Fish Company Inc.]	incransom	Link
2024-02-09	[water.cc]	lockbit3	Link
2024-02-09	[CTSI]	bianlian	Link
2024-02-09	[J.P. Original]	bianlian	Link
2024-02-09	[TechNet Kronoberg AB]	bianlian	Link
2024-02-09	[Capozzi Adler, P.C.]	bianlian	Link
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	Link
2024-02-09	[Grace Lutheran Foundation]	alphv	Link
2024-02-09	[ZGEO]	qilin	Link
2024-02-09	[alfiras.com]	lockbit3	Link
2024-02-09	[wannago.cloud]	qilin	Link
2024-02-09	[grupomoraval.com]	lockbit3	Link
2024-02-09	[cdtmedicus.pl]	lockbit3	Link
2024-02-09	[soken-ce.co.jp]	lockbit3	Link
2024-02-09	[maximumresearch.com]	lockbit3	Link
2024-02-09	[indoramaventures.com]	lockbit3	Link
2024-02-09	[willislease.com]	blackbasta	Link
2024-02-09	[northseayachtsupport.nl]	lockbit3	Link
2024-02-09	[seymourct.org]	lockbit3	Link
2024-02-09	[bsaarchitects.com]	lockbit3	Link
2024-02-09	[moneyadvicetrust.org]	lockbit3	Link
2024-02-09	[posen.com]	abyss	Link
2024-02-09	[macqueeneq.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-09	[parksite.com]	cactus	Link
2024-02-07	[galbusera.it]	lockbit3	Link
2024-02-08	[Ducont]	hunters	Link
2024-02-08	[perkinsmfg.com]	lockbit3	Link
2024-02-08	[originalfootwear.com]	lockbit3	Link
2024-02-08	[Jewish Home Lifecare]	alphv	Link
2024-02-08	[Distecna]	akira	Link
2024-02-07	[Western Municipal Construction]	blacksuit	Link
2024-02-07	[Southwest Binding & Laminating]	blacksuit	Link
2024-02-07	[TeraGo]	akira	Link
2024-02-07	[transaxle.com]	abyss	Link
2024-02-07	[Anderco PTE LTD]	8base	Link
2024-02-07	[Tetrosyl Group Limited]	8base	Link
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	Link
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link
2024-02-06	[axsbolivia.com]	lockbit3	Link
2024-02-06	[vimarequipment.com]	lockbit3	Link
2024-02-06	[deltron.com]	abyss	Link
2024-02-06	[B&B Electric Inc]	bianlian	Link
2024-02-06	[AVer Information]	akira	Link
2024-02-06	[Celeste]	akira	Link
2024-02-06	[ArpuPlus]	medusa	Link
2024-02-06	[gocco.com]	cactus	Link
2024-02-06	[spbglobal.com]	cactus	Link
2024-02-05	[Modern Kitchens]	play	Link
2024-02-05	[Greenwich Leisure]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-05	[Ready Mixed Concrete]	play	Link
2024-02-05	[Northeastern Sheet Metal]	play	Link
2024-02-05	[Hannon Transport]	play	Link
2024-02-05	[McMillan Pazdan Smith]	play	Link
2024-02-05	[Mason Construction]	play	Link
2024-02-05	[Albert Bartlett]	play	Link
2024-02-05	[Perry-McCall Construction]	play	Link
2024-02-05	[Virgin Islands Lottery]	play	Link
2024-02-05	[Premier Facility Management]	play	Link
2024-02-05	[Douglas County Libraries]	play	Link
2024-02-05	[Leaders Staffing]	play	Link
2024-02-06	[asecos.com]	blackbasta	Link
2024-02-05	[GRUPO SCA Release of all data)]	knight	Link
2024-02-05	[themisbourne.co.uk]	lockbit3	Link
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link
2024-02-05	[hutchpaving.com]	lockbit3	Link
2024-02-05	[davis-french-associates.co.uk]	lockbit3	Link
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	Link
2024-02-05	[VCS Observation]	akira	Link
2024-02-05	[noe.wifi.at]	lockbit3	Link
2024-02-05	[ksa-architecture.com]	lockbit3	Link
2024-02-05	[GRTC Transit System]	bianlian	Link
2024-02-05	[semesco.com]	lockbit3	Link
2024-02-05	[ultraflexx.com]	lockbit3	Link
2024-02-05	[tgestiona.br]	lockbit3	Link
2024-02-05	[philogen.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-05	[prima.com]	lockbit3	Link
2024-02-05	[logtainer.com]	lockbit3	Link
2024-02-05	[portline.pt]	lockbit3	Link
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link
2024-02-02	[Innovex Downhole Solutions]	play	Link
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	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.