Cybersecurity Morgenreport

Ausgabe: 20230709

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

Security-News

Heise - Security-Alert

Linux: Sicherheitslücke erlaubt Rechteausweitung, Exploit angekündigt
Im Linux-Kernel schlummert eine Sicherheitslücke, durch die Nutzer ihre Rechte im System ausweiten können. Der Entdecker kündigt Exploit-Code für Ende Juli an.
- Link

Fediverse: Kritische Sicherheitslücken in Mastodon-Software abgedichtet
Betreiber von Mastodon-Instanzen müssen die Server aktualisieren. Ältere Versionen bringen kritische Sicherheitslücken mit, die etwa Codeschmuggel erlauben.
- Link

Cisco Nexus 9000: Angreifer können Verschlüsselung brechen – kein Update
In den Geräten der Nexus-9000-Baureihe von Cisco können Angreifer verschlüsselten Verkehr lesen und verändern. Es gibt weder Software-Update noch Workaround.
- Link

Patchday: Vielfältige Attacken auf Android 11, 12 und 13 möglich
Es gibt wichtige Sicherheitsupdates für verschiedene Android-Versionen. Im schlimmsten Fall könnte Schadcode auf Geräte gelangen.
- Link

Progress schließt weitere kritische Sicherheitslücke in MOVEit Transfer
Mit dem Service Pack für MOVEit Transfer im Juli schließt Progress weitere Sicherheitslücken. Eine davon stuft der Hersteller als kritisch ein.
- Link

Firefox 115 und Thunderbird 102.13 dichten Sicherheitslecks ab
Die Mozilla-Foundation hat Firefox 115, Firefox ESR 115 und Thunderbird 102.13 veröffentlicht. Die neuen Versionen schließen zahlreiche Sicherheitslücken.
- Link

Geräteverwaltung: hochriskante Schwachstelle in Ivanti Endpoint Manager
Eine Sicherheitslücke in der Geräte- und Softwareverwaltung von Ivanti für ChromeOS, Linux, macOS und Windows ermöglicht Angreifern aus dem Netz Codeschmuggel.
- Link

Jetzt patchen! Über 335.000 SSL-VPN-Interfaces von Fortinet attackierbar
Sicherheitsforscher warnen vor weiteren Attacken auf eine kritische Lücke in FortiOS. Patches zum Schließen der Schwachstelle sind seit Wochen verfügbar.
- Link

Sicherheitsupdates: Schadcode-Attacken auf HP-LaserJet-Pro-Drucker möglich
Mehrere LaserJet-Pro-Modelle von HP sind verwundbar. Sicherheitsupdates schaffen Abhilfe.
- Link

Jetzt patchen! Backups von ArcServe UDP durch Admin-Attacke in Gefahr
Es ist ein wichtiges Update für die Backup-Software ArcServe UDP erschienen. Angreifer können sich als Admin Zugang verschaffen.
- Link

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34362	0.940540000	0.987660000	Link
CVE-2023-33246	0.954530000	0.990550000	Link
CVE-2023-27372	0.970730000	0.996380000	Link
CVE-2023-27350	0.971180000	0.996610000	Link
CVE-2023-25717	0.955670000	0.990940000	Link
CVE-2023-21839	0.950530000	0.989620000	Link
CVE-2023-0669	0.964550000	0.993480000	Link

BSI - Warn- und Informationsdienst (WID)

Fri, 07 Jul 2023
Python: Schwachstelle ermöglicht Manipulation [hoch]
Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um HTTP Anfragen zu manipulieren.
- Link

—

Fri, 07 Jul 2023
Python: Schwachstelle ermöglicht Codeausführung [kritisch]
Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 07 Jul 2023
zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Fri, 07 Jul 2023
Apache Kafka: Schwachstelle ermöglicht Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Kafka ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Fri, 07 Jul 2023
dbus: Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen in dbus ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Programmcode mit Administratorrechten auszuführen.
- Link

Fri, 07 Jul 2023
libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff [hoch]
Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

Fri, 07 Jul 2023
libtasn1: Schwachstelle ermöglicht nicht spezifizierten Angriff [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libtasn1 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

Fri, 07 Jul 2023
Python: Schwachstelle ermöglicht Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

Fri, 07 Jul 2023
Samba: Mehrere Schwachstellen ermöglichen Privilegieneskalation [hoch]
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Samba ausnutzen, um seine Privilegien zu erhöhen.
- Link

Fri, 07 Jul 2023
Apache Kafka: Schwachstelle ermöglicht Codeausführung [hoch]
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache Kafka ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

Fri, 07 Jul 2023
Mozilla Firefox: Mehrere Schwachstellen ermöglichen Codeausführung [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um Code auszuführen, Sicherheitsmechanismen zu umgehen, den Benutzer zu täuschen, Informationen offenzulegen und andere unbekannte Effekte zu erzielen.
- Link

Fri, 07 Jul 2023
Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.
- Link

Fri, 07 Jul 2023
VMware Tanzu Spring Framework: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in VMware Tanzu Spring Framework ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.
- Link

Fri, 07 Jul 2023
Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

Fri, 07 Jul 2023
Red Hat OpenShift: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Fri, 07 Jul 2023
Unify OpenScape SBC und Unify OpenScape Branch: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Unify OpenScape SBC und Unify OpenScape Branch ausnutzen, um beliebigen Programmcode auszuführen und Sicherheitsmaßnahmen zu umgehen.
- Link
—
Thu, 06 Jul 2023
Barracuda Networks Email Security Gateway: Schwachstelle ermöglicht Codeausführung [kritisch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Barracuda Networks Email Security Gateway ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 06 Jul 2023
Aruba ArubaOS: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Aruba ArubaOS ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Daten zu manipulieren und Sicherheitsvorkehrungen zu umgehen.
- Link
—
Thu, 06 Jul 2023
ESRI ArcGIS: Mehrere Schwachstellen ermöglichen Cross-Site Scripting [hoch]
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in ESRI ArcGIS ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.
- Link
—
Thu, 06 Jul 2023
Samsung Android: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/8/2023	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2023-188-01)]	critical
7/8/2023	[Debian DLA-3483-1 : nsis - LTS security update]	critical
7/8/2023	[Debian DLA-3484-1 : firefox-esr - LTS security update]	critical
7/8/2023	[Debian DSA-5450-1 : firefox-esr - security update]	critical
7/8/2023	[Rocky Linux 9 : go-toolset and golang (RLSA-2023:3923)]	critical
7/8/2023	[Debian DLA-3487-1 : fusiondirectory - LTS security update]	critical
7/7/2023	[Fedora 37 : firefox (2023-5c979c4971)]	critical
7/7/2023	[Oracle Linux 9 : go-toolset / and / golang (ELSA-2023-3923)]	critical
7/6/2023	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2023-234)]	critical

Datum	Schwachstelle	Bewertung
7/6/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : grpc, protobuf, python-Deprecated, python-PyGithub, python-aiocontextvars, python-avro, python-bcrypt, python-cryptography, python-cryptography-vectors, python-google-api-core, python-googleapis-common-protos, python-grpcio-gcp, python-humanfriendly, python-jsondiff, python-knack, python-opencensus, python-opencensus-context, python-opencensus-ext-threading, python-opentelemetry-api, python-psutil, python-pytest-asyncio, python-requests, python-websocket-client, python-websockets (SUSE-SU-2023:2783-1)]	critical
7/6/2023	[Oracle Global Lifecycle Management (OPatch) (Jan 2023 CPU)]	critical
7/6/2023	[Debian DSA-5447-1 : mediawiki - security update]	critical
7/6/2023	[Progress MOVEit Transfer < 2020.1.11 / 2021.0 < 2021.0.9 / 2021.1 < 2021.1.7 / 2022.0 < 2022.0.7, 2022.1 < 2022.1.8 / 2023.0 < 2023.0.4 Multiple Vulnerabilities (July 2023)]	critical
7/9/2023	[Fedora 38 : perl-CPAN (2023-46924e402a)]	high
7/9/2023	[Fedora 37 : perl-CPAN (2023-1e5af38524)]	high
7/8/2023	[Fedora 38 : python-managesieve (2023-51b4d898bb)]	high
7/8/2023	[Fedora 37 : python-managesieve (2023-d797723a3e)]	high
7/8/2023	[Debian DSA-5449-1 : webkit2gtk - security update]	high
7/8/2023	[SUSE SLES15 / openSUSE 15 Security Update : prometheus-ha_cluster_exporter (SUSE-SU-2023:2799-1)]	high
7/8/2023	[SUSE SLES12 Security Update : bind (SUSE-SU-2023:2793-1)]	high
7/8/2023	[SUSE SLES15 / openSUSE 15 Security Update : prometheus-sap_host_exporter (SUSE-SU-2023:2798-1)]	high
7/8/2023	[SUSE SLES15 / openSUSE 15 Security Update : bind (SUSE-SU-2023:2794-1)]	high
7/8/2023	[Debian DLA-3485-1 : php-cas - LTS security update]	high
7/7/2023	[Fedora 38 : yt-dlp (2023-6b68ed8725)]	high
7/7/2023	[SUSE SLES12 Security Update : bind (SUSE-SU-2023:2789-1)]	high
7/7/2023	[Cisco Firepower Threat Defense Software SNMP DoS (cisco-sa-asaftd-snmp-dos-qsqBNM6x)]	high
7/7/2023	[Cisco Adaptive Security Appliance Software SNMP DoS (cisco-sa-asaftd-snmp-dos-qsqBNM6x)]	high
7/7/2023	[NVIDIA DGX A100/A800 System BIOS < 1.21 Multiple Vulnerabilities]	high
7/7/2023	[Azure DevOps Server 2022 XSS]	high
7/7/2023	[Openfire Authentication Bypass (CVE-2023-32315)]	high
7/6/2023	[FreeBSD : electron{23,24} – multiple vulnerabilities (d1681df3-421e-4a63-95b4-a3d6e29d395d)]	high
7/6/2023	[FreeBSD : gitea – avoid open HTTP redirects (8ea24413-1b15-11ee-9331-570525adb7f1)]	high
7/6/2023	[HP LaserJet Printers DoS (HPSBPI03852)]	high

Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2023-07-07	Université de l'Ouest de l'Écosse (UWS)	[GBR]	Link
2023-07-07	Bureau du Procureur Général et le Ministère des Affaires Juridiques de Trinité-et-Tobago (AGLA)	[TTO]	Link
2023-07-07	Jackson Township	[USA]	Link
2023-07-06	Commission électorale du Pakistan (ECP)	[PAK]	Link
2023-07-05	Hôpital universitaire Luigi Vanvitelli de Naples	[ITA]	Link
2023-07-04	Nagoya Port Transport Association	[JPN]	Link
2023-07-04	Roys of Wroxham	[GBR]	Link
2023-07-04	ibis acam	[AUT]	Link
2023-07-02	Aéroport de Montpellier	[FRA]	Link
2023-07-02	Ville d'Agen	[FRA]	Link

Quellen

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/

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.