Ausgabe: 20230707

Security-News

Heise - Security-Alert

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
—
Sicherheitsupdate: Attacken auf WordPress-Plug-in Ultimate Member
Derzeit nutzen Angreifer eine kritische Lücke im WordPress-Plug-in Ultimate Member aus. Der Anbieter rät zu einem zügigen Update.
- Link
—
Nvida: Treiber-Updates gegen Sicherheitslücken
Nvidias Grafikkartentreiber für Linux und Windows haben hochriskante Sicherheitslücken. Der Hersteller liefert jetzt Aktualisierungen zum Abdichten der Lecks.
- Link
—
Sicherheitsupdates: Dell-BIOS gegen verschiedene Attacken gerüstet
Wer einen Computer von Dell besitzt, sollte das BIOS aus Sicherheitsgründen auf den aktuellen Stand bringen.
- 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-2023-33246	0.938880000	0.987420000	Link
CVE-2023-28771	0.905600000	0.983580000	Link
CVE-2023-27372	0.971410000	0.996710000	Link
CVE-2023-27350	0.969310000	0.995690000	Link
CVE-2023-26360	0.900700000	0.983180000	Link
CVE-2023-25717	0.911550000	0.984100000	Link
CVE-2023-23397	0.939930000	0.987550000	Link
CVE-2023-21839	0.951150000	0.989780000	Link
CVE-2023-21716	0.923940000	0.985350000	Link
CVE-2023-21554	0.919580000	0.984840000	Link
CVE-2023-0669	0.966160000	0.994160000	Link

BSI - Warn- und Informationsdienst (WID)

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
—
Thu, 06 Jul 2023
Progress Software MOVEit: Mehrere Schwachstellen [hoch]
Ein Angreifer kann mehrere Schwachstellen in Progress Software MOVEit ausnutzen, um Daten zu manipulieren oder einen Denial of Service zu verursachen.
- Link
—
Thu, 06 Jul 2023
Android Patchday Juli 2023 [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Thu, 06 Jul 2023
GitLab: Schwachstelle ermöglicht Privilegieneskalation [hoch]
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in GitLab ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Thu, 06 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 Angriff durchzuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Thu, 06 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 Angriff durchzuführen, einen nicht näher spezifizierten Angriff durchzuführen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.
- Link
—
Thu, 06 Jul 2023
Red Hat OpenShift: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen Informationen offenzulegen oder einen Denial of Service zu verursachen.
- Link
—
Thu, 06 Jul 2023
Linux Kernel (ksmbd): Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.
- Link
—
Thu, 06 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
—
Thu, 06 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 Sicher-

heitsvorkehrungen zu umgehen.
- Link
—
Thu, 06 Jul 2023
PCRE (Perl Compatible Regular Expressions): Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PCRE (Perl Compatible Regular Expressions) ausnutzen, um einen Denial of Service Angriff durchzuführen und um Informationen offen zu legen.
- Link
—
Thu, 06 Jul 2023
D-LINK Access Point (AP) DAP-2622: Schwachstelle ermöglicht Codeausführung [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle im D-LINK Access Point (AP) Modell DAP-2622 ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Wed, 05 Jul 2023
python-cryptography: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in python-cryptography ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link
—
Wed, 05 Jul 2023
Fabasoft Folio und Fabasoft Cloud: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Fabasoft Folio und Fabasoft Cloud ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsmaßnahmen zu umgehen.
- Link
—
Wed, 05 Jul 2023
HPE ProLiant: Schwachstelle ermöglicht Codeausführung [hoch]
Ein Angreifer kann eine Schwachstelle in HPE ProLiant ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Wed, 05 Jul 2023
cURL: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um das System zum Absturz zu bringen, um Informationen aus den Cookies offenzulegen, um dem Benutzer falsche Informationen darzustellen und sich als ein Benutzer auszugeben.
- Link
—
Wed, 05 Jul 2023
libcurl: Schwachstelle ermöglicht Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libcurl ausnutzen, um einen Denial of Service Angriff durchzuführen oder auf Daten zuzugreifen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/6/2023	[Fedora 38 : kernel (2023-2846d5650e)]	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
7/5/2023	[Nuxt.js 3.4.x < 3.4.3 Remote Code Execution]	critical
7/5/2023	[Fedora 38 : firefox (2023-b9b15ebaad)]	critical
7/5/2023	[Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6201-1)]	critical
7/5/2023	[Ubuntu 22.04 LTS : CPDB vulnerability (USN-6204-1)]	critical
7/4/2023	[EulerOS 2.0 SP11 : apr (EulerOS-SA-2023-2282)]	critical
7/4/2023	[EulerOS 2.0 SP11 : emacs (EulerOS-SA-2023-2288)]	critical
7/4/2023	[EulerOS 2.0 SP11 : httpd (EulerOS-SA-2023-2295)]	critical
7/4/2023	[EulerOS 2.0 SP11 : haproxy (EulerOS-SA-2023-2293)]	critical
7/4/2023	[EulerOS 2.0 SP11 : curl (EulerOS-SA-2023-2262)]	critical
7/4/2023	[EulerOS 2.0 SP11 : haproxy (EulerOS-SA-2023-2269)]	critical
7/6/2023	[Debian DSA-5448-1 : linux - security update]	high
7/6/2023	[Debian DLA-3479-1 : golang-yaml.v2 - LTS security update]	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
7/5/2023	[Fedora 37 : python-reportlab (2023-3b82f4aa86)]	high
7/5/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : qt6-base (SUSE-SU-2023:2780-1)]	high
7/5/2023	[SUSE SLES15 Security Update : dnsdist (SUSE-SU-2023:2777-1)]	high
7/5/2023	[SUSE SLES15 / openSUSE 15 Security Update : rmt-server (SUSE-SU-2023:2781-1)]	high
7/5/2023	[SUSE SLES15 / openSUSE 15 Security Update : kubernetes1.18 (SUSE-SU-2023:2773-1)]	high
7/5/2023	[openSUSE 15 Security Update : virtualbox (openSUSE-SU-2023:0166-1)]	high
7/5/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2782-1)]	high
7/5/2023	[GitLab 12.8 < 15.11.11 / 16.0 < 16.0.7 / 16.1 < 16.1.2 (CVE-2023-3484)]	high
7/5/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Django vulnerability (USN-6203-1)]	high
7/5/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 22.10 / 23.04 : containerd vulnerabilities (USN-6202-1)]	high
7/5/2023	[FreeBSD : Gitlab – Vulnerabilities (d8972bcd-1b64-11ee-9cd6-001b217b3468)]	high
7/4/2023	[EulerOS 2.0 SP11 : git (EulerOS-SA-2023-2289)]	high
7/4/2023	[EulerOS 2.0 SP11 : golang (EulerOS-SA-2023-2292)]	high
7/4/2023	[EulerOS 2.0 SP11 : kernel (EulerOS-SA-2023-2272)]	high
7/4/2023	[EulerOS 2.0 SP11 : openssl (EulerOS-SA-2023-2275)]	high
7/4/2023	[EulerOS 2.0 SP11 : samba (EulerOS-SA-2023-2300)]	high

Datum	Schwachstelle	Bewertung
7/4/2023	[EulerOS 2.0 SP11 : git (EulerOS-SA-2023-2265)]	high
7/4/2023	[EulerOS 2.0 SP11 : harfbuzz (EulerOS-SA-2023-2270)]	high
7/4/2023	[EulerOS 2.0 SP11 : less (EulerOS-SA-2023-2273)]	high

Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2023-07-05	Hôpital universitaire Luigi Vanvitelli de Naples	[ITA]	Link
2023-07-04	Nagoya Port Transport Association	[JPN]	Link
2023-07-02	Aéroport de Montpellier	[FRA]	Link
2023-07-02	Ville d'Agen	[FRA]	Link

Quelle: Cyberwatch

Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-07-07	[Kenya Bureau Of Standards]	rhysida	Link
2023-07-07	[Lazer Tow]	play	Link
2023-07-07	[Star Island Resort]	play	Link
2023-07-07	[Indiana Dimension]	play	Link
2023-07-07	[Lawer SpA]	play	Link
2023-07-06	[DELARUE.COM]	clop	Link
2023-07-06	[ENERGYTRANSFER.COM]	clop	Link
2023-07-06	[PAYCOR.COM]	clop	Link
2023-07-06	[NETSCOUT.COM]	clop	Link
2023-07-06	[WOLTERSKLUWER.COM]	clop	Link
2023-07-06	[CADENCEBANK.COM]	clop	Link
2023-07-06	[BANKWITHUNITED.COM]	clop	Link
2023-07-06	[NEWERATECH.COM]	clop	Link
2023-07-06	[NST Attorneys at Law]	play	Link
2023-07-06	[Uniquify]	play	Link
2023-07-06	[Geneva Software]	play	Link
2023-07-06	[MUJI Europe Holdings Limited]	play	Link
2023-07-06	[Betty Lou's]	play	Link
2023-07-06	[Capacity LLC]	play	Link
2023-07-06	[Safety Network]	play	Link
2023-07-06	[Carvin Software]	bianlian	Link
2023-07-06	[Ella Insurance Brokerage]	bianlian	Link
2023-07-06	[betalandservices.com]	lockbit3	Link
2023-07-06	[chasc.org]	lockbit3	Link
2023-07-06	[cls-group.com]	lockbit3	Link
2023-07-06	[gacegypt.net]	lockbit3	Link
2023-07-06	[siegfried.com.mx]	lockbit3	Link
2023-07-06	[Pinnergy]	akira	Link
2023-07-06	[Bangladesh Krishi Bank]	alphv	Link
2023-07-06	[ASIC Soluciones]	qilin	Link
2023-07-06	[KIRWIN FRYDAY MEDCALF Lawyers LLP]	8base	Link
2023-07-05	[TRANSPERFECT.COM]	clop	Link
2023-07-05	[QUORUMFCU.ORG]	clop	Link
2023-07-05	[MERATIVE.COM]	clop	Link
2023-07-05	[NORGREN.COM]	clop	Link
2023-07-05	[CIENA.COM]	clop	Link
2023-07-05	[KYBURZDRUCK.CH]	clop	Link
2023-07-05	[UNITEDREGIONAL.ORG]	clop	Link
2023-07-05	[TDECU.ORG]	clop	Link
2023-07-05	[BRADYID.COM]	clop	Link
2023-07-05	[BARRICK.COM]	clop	Link
2023-07-05	[DURR.COM]	clop	Link
2023-07-05	[ZooTampa at Lowry Park]	blacksuit	Link
2023-07-05	[Avalign Technologies]	blackbyte	Link
2023-07-05	[Portugal Scotturb Data Leaked]	ragnarlocker	Link
2023-07-03	[guestgroup.com.au]	lockbit3	Link
2023-07-05	[Murphy]	akira	Link
2023-07-05	[eurosupport.com]	lockbit3	Link
2023-07-05	[recamlaser.com]	lockbit3	Link
2023-07-05	[mitr.com]	lockbit3	Link
2023-07-04	[Hoosier Equipment company]	medusalocker	Link
2023-07-04	[Yunus Emre Institute Turkey]	medusa	Link
2023-07-04	[Polanglo]	8base	Link
2023-07-03	[Jefferson County Health Center]	karakurt	Link
2023-07-03	[snjb.net]	lockbit3	Link
2023-07-03	[oneexchangecorp.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-07-03	[Townsquare Media Inc]	alphv	Link
2023-07-03	[Ayuntamiento de Arganda City Council]	rhysida	Link
2023-07-03	[Duncan Disability Law]	alphv	Link
2023-07-03	[Hollywood Forever]	rhysida	Link
2023-07-03	[Mutuelle LMP]	medusa	Link
2023-07-03	[Luna Hotels & Resorts]	medusa	Link
2023-07-03	[BM GROUP POLYTEC S.p.A.]	rhysida	Link
2023-07-03	[Brett Martin]	blackbyte	Link
2023-07-02	[blowtherm.it]	lockbit3	Link
2023-07-02	[Ucamco Belgium]	medusalocker	Link
2023-07-01	[Ashley HomeStore]	mallox	Link
2023-07-01	[Blount Fine Foods]	blackbasta	Link
2023-07-01	[Blount]	blackbasta	Link
2023-07-01	[DVA - DVision Architecture]	ransomexx	Link
2023-07-01	[Kondratoff Persick LLP]	bianlian	Link
2023-07-01	[Undisclosed Staffing Company]	bianlian	Link

Quelle: Ransomwatch