"Mythbuster"-Projekt
A user study on CSAF

30. DFN-Konferenz
"Sicherheit in vernetzten Systemen"

Janik Aurich, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
Julia Wunder, FAU
Martin Waleczek, DFN-CERT

waleczek@dfn-cert.de

Mythbuster

Projekt und Partner

Realistische Bewertung von Sicherheitsmaßnahmen unter Einbeziehung des Faktors Mensch

https://projekt-mythbuster.de/

Mythbuster

Fragestellung als Beispiel

Ist es sinnvoll, von den Mitarbeitenden regelmäßige Passwortwechsel vornehmen zu lassen?

Mythbuster

Fragestellung als Beispiel

Ist es sinnvoll, von den Mitarbeitenden regelmäßige Passwortwechsel vornehmen zu lassen?

Oder könnten die Kosten für den Support bei vergessenen Passwörtern den angemessenen Rahmen übersteigen, weil die zu schützenden Daten gar nicht so sensibel sind?

Mythbuster

Zielvorstellung DFN-CERT

VO

Ziel für das DFN-CERT ist es im Projekt Mythbuster, Inhalt und Sinnhaftigkeit der eigenen Sicherheitsdienstleistungen kritisch zu prüfen, unter neuen Gesichtspunkten zu bearbeiten und aus Kundensicht zu verbessern. Bei welchen der angebotenen Sicherheitsdienstleistungen besteht Verbesserungsbedarf?

Es ist mir nicht möglich, spezifische Informationen über den Bedarf an Verbesserungen der von DFN-CERT angebotenen Sicherheitsdienstleistungen bereitzustellen, da keine konkreten Informationen darüber vorliegen. Es wäre wahrscheinlich am besten, direkt an DFN-CERT zu fragen, um die aktuellsten Informationen zu erhalten.

Schwachstelleninformationen

Schwachstelleninformationsdienst für das DFN

Anwender sollen proaktiv über mögliche Schwachstellen in eingesetzten Produkten informiert werden.

- fast der gesamte Softwarekatalog gängiger Linux-Distributionen
  - Debian, Fedora, Red Hat, Oracle, SUSE, Ubuntu,…
- verbreitete Betriebssysteme auf Patchtagsbasis
  - Android, Apple, Microsoft,…
- Hersteller von Netzwerkkomponenten
  - Aruba, Cisco, F5, Fortinet, Juniper,…
- einzelne gängige Anwendungen
  - Adobe, Chrome, Firefox, Foxit, Thunderbird…

Schwachstelleninformationen

Bewertung I - DAF

Dringlichkeit / Eintrittspotenzial

Eintrittspotenzial	Verbreitungsmethode		
Status der Schwachstelle	manuell	automatisch	replizierend
theoretisch	sehr gering	gering	mittel
ausnutzbar	gering	mittel	hoch
aktiv	mittel	hoch	hoch
Exploit veröffentlicht	mittel	hoch	sehr hoch

Schadenspotenzial

Schadenspotenzial	Kontext			
Verlust	Benutzer	Dienst	System	Netzwerk
Übernahme der Kontrolle	hoch	hoch	sehr hoch	sehr hoch
Übernahme von Berechtigungen	mittel	mittel	hoch	hoch
Integrität	gering	mittel	hoch	hoch
Vertraulichkeit	sehr gering	gering	mittel	hoch
Verfügbarkeit	sehr gering	gering	mittel	hoch
Umgehung von Sicherheitsmaßnahmen	sehr gering	gering	mittel	hoch

aktuelles Schadenspotenzial

aktuelles Schadenspotenzial	Schadenspotenzial				
Eintrittspotenzial	sehr gering	gering	mittel	hoch	sehr hoch
sehr gering	sehr gering	sehr gering	gering	gering	mittel
gering	sehr gering	gering	gering	mittel	hoch
mittel	gering	gering	mittel	hoch	hoch
hoch	gering	mittel	hoch	hoch	sehr hoch
sehr hoch	mittel	hoch	hoch	sehr hoch	sehr hoch

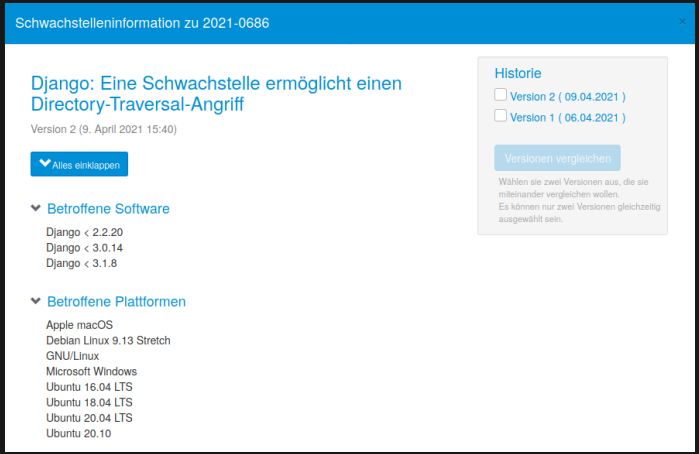
Schwachstelleninformationen

Bewertung II - CVSS

None: 0.0, Low: 0.1 - 3.9, Medium: 4.0 - 6.9, High: 7.0 - 8.9, Critical: 9.0 - 10.0

Schwachstelleninformationen

Beispiel



Schwachstelleninformationen

Beispiel

Risikobewertung

Gesamtbewertung des Risikos:	mittel
CVSS Base Score:	4.3
CVSS Exploitability:	2.8
CVSS Impact:	1.4
CVSS Temporal:	3.9

Beschreibung

Ein Angreifer kann eine Schwachstelle aus der Ferne ausnutzen, um einen Directory-Traversal-Angriff durchzuführen. Für die Ausnutzung der Schwachstelle sind übliche Privilegien erforderlich.

Der Hersteller bestätigt die Schwachstelle und veröffentlicht zu die Versionen 3.1.8, 3.0.14, und 2.2.20 als Sicherheitsupdates.

Canonical stellt für Ubuntu 20.10, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS und Ubuntu 16.04 LTS Sicherheitsupdates für 'python-django' zur Behebung der Schwachstelle zur Verfügung.

Lösung

Django Security Releases 3.1.8, 3.0.14, 2.2.20
https://www.djangoproject.com/weblog/2021/apr/06/security-releases/

Ubuntu Security Notice USN-4902-1
https://ubuntu.com/security/notices/USN-4902-1

Debian LTS Security Advisory DLA 2622-1
https://lists.debian.org/debian-lts-announce/2021/04/msg00008.html

Schwachstelleninformationen

Beispiel

Workaround

Keine Informationen vorhanden.

Schwachstellen

CVE-2021-28658: Schwachstelle in Django ermöglicht Directory-Traversal-Angriff

Es existiert eine Schwachstelle im 'MultiPartParser' von Django, die über das Hochladen von Dateien mit einem speziell angepassten Namen einen Directory-Traversal-Angriff ermöglicht.

Referenzen

Patches:

Django Security Releases 3.1.8, 3.0.14, 2.2.20:
https://www.djangoproject.com/weblog/2021/apr/06/security-releases/
Ubuntu Security Notice USN-4902-1:
https://ubuntu.com/security/notices/USN-4902-1
Debian LTS Security Advisory DLA 2622-1:
https://lists.debian.org/debian-lts-announce/2021/04/msg00008.html

Zusätzliche Informationen:

Schwachstelle CVE-2021-28658 (NVD):
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28658

Historie

9. April 2021 15:40:

Für Debian 9 Stretch (LTS) steht ein Sicherheitsupdate zur Behebung der Schwachstelle in 'python-django' zur Verfügung.

6. April 2021 17:11:

Neues Advisory

Schwachstelleninformationen

Anhang


```
{
  "ref_num": "2021-0686",
  "version": 2,
  "fieldsets": {
    "basic": {
      "created": "20210406T15:10:12",
      "title": "Django: Eine Schwachstelle erm\u00f6glicht einen Directory-Traversal-Angriff",
      "description": "Ein Angreifer kann eine Schwachstelle aus der Ferne ausnutzen, um einen Directory-Traversal-Angriff
      "workaround": null,
      "history": [
        {
          "version": "2",
          "timestamp": "20210409T15:40:20",
          "description": "F\u00fcr Debian 9 Stretch (LTS) steht ein Sicherheitsupdate zur Behebung der Schwachstelle in '
        },
        {
          "version": "1",
          "timestamp": "20210406T17:11:16",
          "description": "Neues Advisory"
        }
      ],
      "references": [
        {
          "type": "patch",
          "url": "https://www.djangoproject.com/weblog/2021/apr/06/security-releases/",
          "description": "Django Security Releases 3.1.8, 3.0.14, 2.2.20"
        },
        {
          "type": "patch",
          "url": "https://ubuntu.com/security/notices/USN-4902-1",
          "description": "Ubuntu Security Notice USN-4902-1"
        },
        {
          "type": "info",
          "url": "http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28658",
          "description": "Schwachstelle CVE-2021-28658 (NVD)"
        },
        {
          "type": "patch",
          "url": "https://lists.debian.org/debian-lts-announce/2021/04/msg00008.html",
          "description": "Debian LTS Security Advisory DLA 2622-1"
        }
      ],
```

Schwachstelleninformationen

Anhang


```
    "vulnerabilities": [
      {
        "name": "CVE-2021-28658",
        "title": "Schwachstelle in Django erm\u00f6glicht Directory-Traversal-Angriff",
        "description": "Es existiert eine Schwachstelle im 'MultiPartParser' von Django, die \u00fcber das Hochladen vo
      }
    ]
  },
  "scoring": {
    "daf": {
      "risk": "medium"
    },
    "cvss3": {
      "base_score": "4.3",
      "exploitability_score": "2.8",
      "impact_score": "1.4",
      "temporal_score": "3.9",
      "vector": "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C"
    },
    "cpes": [
      {
        "cpe": "cpe:/a:djangoproject:django:2.2.20",
        "relation": "<",
        "type": "software",
        "displayname": "Django < 2.2.20"
      },
      {
        "cpe": "cpe:/a:djangoproject:django:3.0.14",
        "relation": "<",
        "type": "software",
        "displayname": "Django < 3.0.14"
      },
      {
        "cpe": "cpe:/a:djangoproject:django:3.1.8",
        "relation": "<",
        "type": "software",
        "displayname": "Django < 3.1.8"
      },
      {
```

Common Security Advisory Format

Probleme und Lösungsansatz über CSAF

- Anzahl veröffentlichter Schwachstellen steigt kontinuierlich
- Anzahl eingesetzter Produkte (Hardware, Software, Firmware) bestimmt Anzahl zu verarbeitender Advisories

  Schwachstelleninformationen werden meist manuell verarbeitet

CSAF will den Zeitrahmen zwischen Veröffentlichung eines Patches und Aktion vor Ort minimieren

- Automatisierung, maschinenverarbeitbar (JSON)

  CSAF ist Nachfolger von CVRF

  CSAF 2.0 vs CVRF 1.2: https://github.com/oasis-tcs/csaf/issues/127
- Automatisches Abholen von Herstelleradvisories

  üblicherweise verschiedenste Formate: txt, JSON, .doc, PDF,…
- Abgleich mit Asset-Datenbank

Common Security Advisory Format

Beteiligte Industriepartner

1. AT&T
2. Cisco
3. Microsoft
4. Red Hat
5. Oracle
6. Siemens
7. BSI

Common Security Advisory Format

Struktur von CSAF-Meldungen

1. Metadata

   ID, Status, Datum, Referenzen, …

2. Produktbaum

   CPEs, alle im Dokument verwendeten Produkte, …

3. Schwachstellen

   ID, Scores, Gegenmaßnahmen, …

Common Security Advisory Format

Einführung von CSAF für Schwachstelleninformationen des DFN-CERT

VO

Sollte das DFN-CERT vor der Einführung von CSAF eine Nutzerbefragung zum bisherigen Advisory-Format durchführen, die in einer Masterarbeit bearbeitet wird?

Ja, es wäre sinnvoll, vor der Einführung von CSAF eine Nutzerbefragung zum bisherigen Advisory-Format durchzuführen. Hierbei können die Meinungen, Anforderungen und Bedürfnisse der Anwender des DFN-CERT erfasst werden. So kann das DFN-CERT sicherstellen, dass die Einführung von CSAF tatsächlich eine Verbesserung für die Anwender darstellt und dass die Übergangspfade und -unterstützung angemessen sind.

Eine solche Nutzerbefragung kann auch als Masterarbeit bearbeitet werden, um zu untersuchen, ob CSAF tatsächlich eine bessere Lösung für die Anwender des DFN-CERT ist. Die Ergebnisse der Befragung können dem DFN-CERT bei der Entscheidung helfen, ob CSAF eingeführt werden sollte und wie die Übergangspfade gestaltet werden sollten.

A user study on CSAF, evaluating factors that drive adoption of security advisory standards

Master Thesis von Janik Aurich, FAU

Forschungsfragen:

1. Welche Faktoren begünstigen die Annahme neuer Sicherheitsstandards?
2. Welche dieser Kriterien werden im CSAF berücksichtigt?
3. Welche Rolle spielt dabei die mögliche Automatisierung (Benutzer- und Herstellerseite)?
4. Wieviele Ressourcen werden durchschnittlich für die Verarbeitung von Sicherheitshinweisen benötigt?

A user study on CSAF

Master Thesis von Janik Aurich, FAU

Bestimmende Faktoren:

	Informationssammlung (Quellen)	Informationsverarbeitung (Automatisierung)	Entscheidungsfindung / Aktion (Handlungsempfehlung)
Methoden (means)	Suche Benachrichtigung	existierende Werkzeuge manuelle Arbeit	empfundenes Risiko Zuständigkeit Ressourcen
Notwendigkeiten (needs)	Relevanz Verfügbarkeit	ausreichende Informationen Maschinenlesbarkeit	Zusammenfassung Überblick
Hindernisse (pains)	Anzahl Umfang	Redundanz Komplexität	Verfügbarkeit Richtlinien
Optionales (wants)	Sicherheit Vertrauen Zeit	Sprache Filterung / Sortierung Zeit	Austausch Risikobewertung

Danke

für die Aufmerksamkeit

Falls Sie Interesse haben, an der Verbesserung der Schwachstelleninformationen mitzuarbeiten:

Sprechen Sie mich an!