#sicherheit

Kritische Infrastrukturen vertrauen auf PSIM. Wir haben es gehackt!

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e.V.

CONCEPTURE

Inhalt

1 Was sind KRITIS?

Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

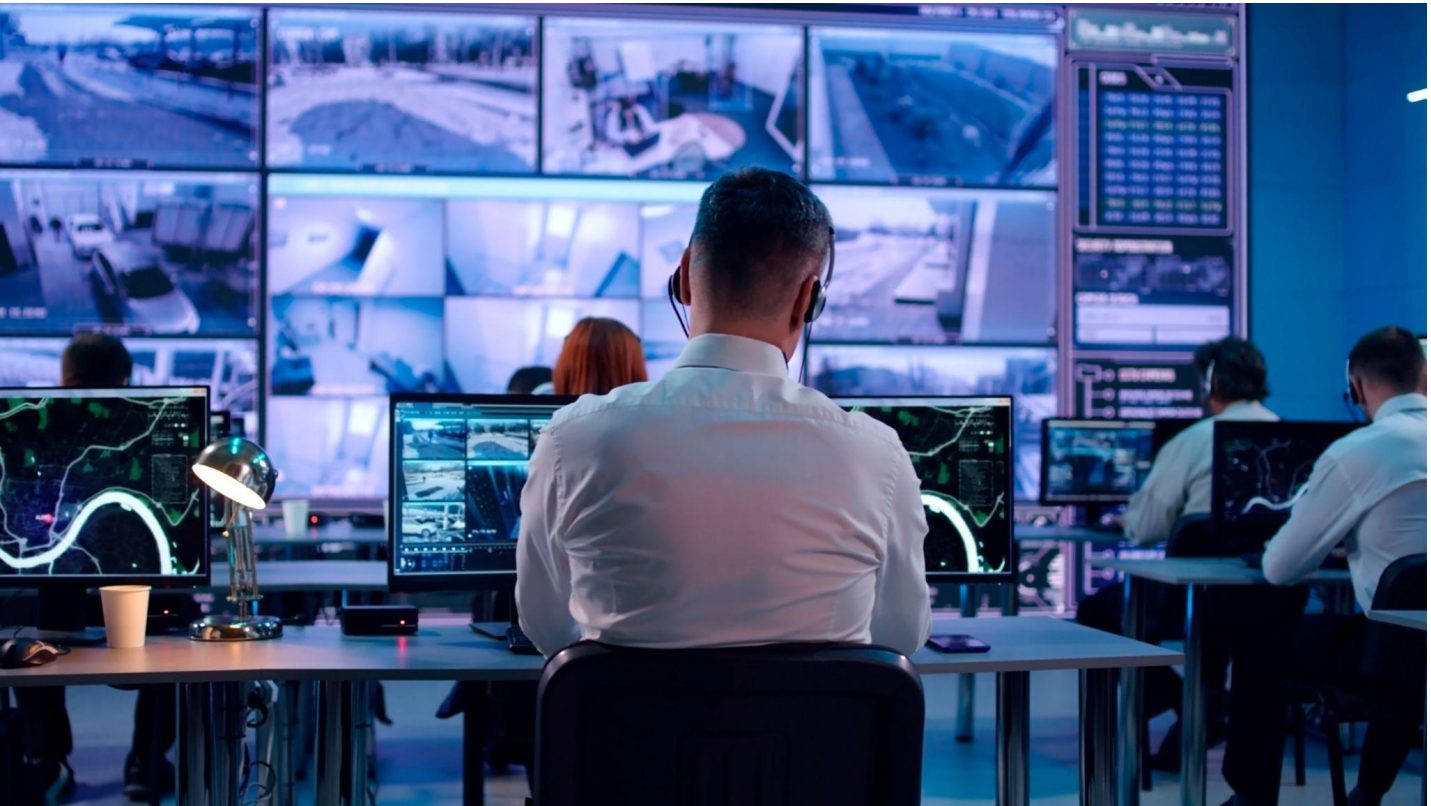
2 Sicherheitstechnik & PSIM

Häufig integrierte Systeme

- Videoüberwachung
- Bewegungsmelder
- Glasbruchsensoren
- Kartenleser (Zutrittskontrolle)
- Zaunsicherung (Detektoren)
- ELA / SAA
- Schranken & Poller
- Schließsysteme
- Fluchttürterminal
- Brandmelder
- Intercom
- PNA (Personennotruf)
- Klima, Lüftung, Heizung
- Jalousiesteuerung
- Lichtsteuerung
- Aufzugssteuerung
- Gebäudeleittechnik
- Produktionstechnik
- Maschinen- und Anlagentechnik

2 Sicherheitstechnik & PSIM

Die Sicherheitsleitstelle



Unterschiedlichste Sicherheitssysteme werden zentral überwacht und gesteuert

2 Sicherheitstechnik & PSIM

Sicherheitsmanagement in der Peripherie

...das kann auch mal so aussehen 😅

3 Sicherheitsanalyse Winguard

winguard always retain control ist ein herstellerneutrales Gefahrenmanagementsystem (GMS/PSIM) der Firma Advancis

Als zentrales System für kritische Prozesse, wie z.B. Zutrittskontrollen oder der Betrieb der Brandmeldeanlage hat Winguard einen erhöhten IT-Sicherheitsschutzbedarf

In der Werbebroschüre wird das aufgegriffen, so ist z.B. die Rede von:

- *Eingesetzter Verschlüsselung (TLS und AES)*
- *Möglichkeit der Redundanz*

Um diese Aussagen zur Sicherheit zu prüfen, wurde WinGuard auf mögliche Schwachstellen untersucht.

- *Dabei wurden Sicherheitsprobleme, die nicht praxisrelevant sind ignoriert (z.B. information disclosure https://cwe.mitre.org/data/definitions/200.html)*

3 Sicherheitsanalyse Winguard

Versuchsaufbau

Die Herausforderung besteht in einer möglichst realistischen Nachstellung eines Angriffs

- Blackbox Test
  - Der Angreifer hat keine Kenntnis über den Quellcode
- Nutzen der öffentlich verfügbaren Dokumentation
- Lokale WinGuard Installation
  - Ein Angreifer wird kein großes Testnetzwerk mit verschiedensten Schnittstellen zur Verfügung haben

Prämisse: Der Angreifer kann mit dem WinGuard Server kommunizieren.

3 Sicherheitsanalyse Winguard

Erster Ansatz

Untersuchung der verschiedenen Module, die WinGuard unterstützt, jedoch:

- Mehr als 100 Module für verschiedenste Systeme
- Genutzte Module variieren stark
- Ein Angreifer müsste für den Großteil der Module über eine Sicherheitslücke verfügen, um flexible Winguard Installationen anzugreifen

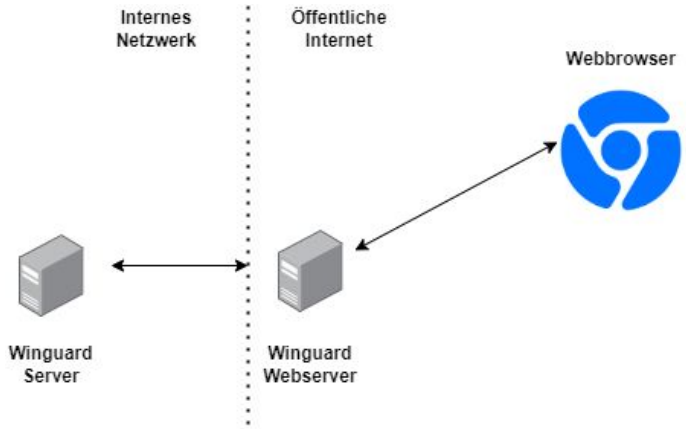
Daher Konzentration auf Schnittstellen zur Steuerung von Winguard (Webserver, Serviceschnittstelle etc.)

4 Finding 1: Webserver

Erstes Ziel: Untersuchung des WinGuard Webserver für die WinGuard Webapp

Grund: Webserver sind klassischerweise nach außen exponiert und ein Angreifer könnte daher Schaden anrichten (ohne im internen Netz zu sein).

Versuchsaufbau

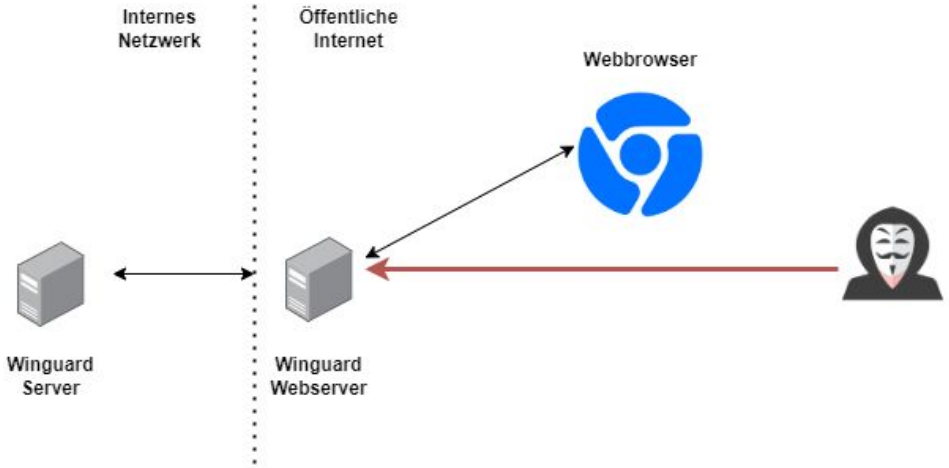


Winguard Server und Winguard Webserver sind voneinander getrennte Prozesse. Diese können z.B. auf getrennten Systemen betrieben werden.

4 Finding 1: Webserver

Vorgehen

Ein Angreifer würde also nicht direkt den Winguard Server angreifen, sondern den Winguard Webserver



4 Finding 1: Webserver

Ziel: Winguard Webserver

- Webserver liefert wie gewöhnlich Dateien für die WebApp aus JS/HTML/CSS…
- Zusätzlich stellt der Webserver einen “Websocket” Server bereit
- Die Webanwendung wird also durch den Webserver ausgeliefert Anschließend kommuniziert die Webanwendung dann mit dem “Websocket” Server. Beispiel:

{"method":"login","params":{"username":"Benuter1", "password":"Geheim","language":"de","workstation": "Web","type":"web"},"Id":3}

4 Finding 1: Webserver - Denial of Service

Denial of Service über Websocket

- Ist der Webserver nicht erreichbar erhält der Bediener keinen Zugriff auf Winguard
- “Klassischer” Ansatz
  - Angreifer sendet Millionen von nutzlosen Anfragen
    Web Server ist ausgelastet, kein Zugriff mehr für reguläre Benutzer möglich.

  Dabei gibt es für den Angreifer aber folgende Probleme:
  - Der Angreifer muss über eine sehr gute Netzwerkanbindung verfügen (besser als das angegriffene System)
  - IP des Angreifers kann einfach gesperrt werden (z.B. in der Firewall)
    - Auslastung geht sofort wieder auf 0 und der Webserver ist für Benutzer wieder normal erreichbar

4 Finding 1: Webserver - Denial of Service

Denial of Service über Websocket

- Es findet sich jedoch ein Fehler in der Websocket Funktion:
  {"method":"GetSettings","params":{"keys":[]....
- Der Winguard Server führt den Befehl wie folgt aus:

```
foreach (string key1 in keys)
{
  string key = key1;
  AppSetting appSetting = this.WebCfg.AppSettings.Where<AppSetting>((Func<AppSetting, bool>) (g => g.Name.ToLower() == key.ToLower())).FirstOrDefault<App
  if (appSetting != null && (!appSetting.AuthorizationRequired || this.IsAuthorized))
```

- Das Problem ist hier, dass kein Length-Check des Parameters “Keys” vorgenommen wird. Dadurch ist ein Denial of Service möglich.

4 Finding 1: Webserver - Denial of Service

Denial of Service über Websocket

- Sendet der Angreife viele leere Keys werden diese ohne Überprüfung durch WinGuard in den Speicher geladen und dort vorgehalten
  - Aufgrund der Winguard Speicherstruktur genügt es, wenn der Angreifer wenige MB Daten sendet um den Speicher komplett zu füllen

- Die anfänglich beschriebenen “klassischen” Probleme eines Denial of Service werden aus der Sicht des Angreifers damit gelöst
  - Netzwerkanbindung des Angreifers spielt nun keine Rolle mehr (Die wenigen MB Daten lassen sich auch z.B. über das Mobilfunknetz übertragen)
  - IP Sperrung des Angreifers löst das Problem nicht, da die Daten einmalig gesendet wurden, folglich bleibt das WinGuard System ausgelastet.

4 Finding 1: Webserver - Denial of Service

Denial of Service über Websocket, praktisches Beispiel

Auslastung im Normalbetrieb:

Name	Status	CPU	Arbeitss...	Datenträ...	Netzwerk	GPU	GPU-Modul	Stromverbrauch	Stromverbrau...
Webserver		0%	15,4 MB	0 MB/s	0 MBit/s	0%		Sehr niedrig	Sehr niedrig

- Sehr geringe Systemauslastung, nur wenige MB Arbeitsspeicher (Auf dem Testsystem stehen ~ 4000mb zur Verfügung)
- Kaum CPU Last

Nach einem Angriff:

Name	Status	CPU	Arbeitss...	Datenträ...	Netzwerk	GPU	GPU-Modul	Stromverbrauch	Stromverbrau...
Webserver		71,6%	4.172,3 MB	0 MB/s	0 MBit/s	0%		Sehr hoch	Hoch

- Angreifer sendete einmalig weniger als 300mb Daten, System ist einige Minuten sehr ausgelastet

5 Finding 2: WinGuard Service Zugang

WinGuard Service Zugang

Neben dem Webserver, gibt es noch einen Service-Zugang, der während der Suche nach Schwachstellen aufgefallen ist.

Ist diese Schnittstelle in der Konfiguration aktiviert, ergaben sich mehrere Sicherheitsprobleme

5 Finding 2: WinGuard Service Zugang - Passwort Brute Force

Passwort Brute Force

- Über WinGuard Einstellungen lässt sich ein Schutz vor Brute-Force-Angriffen (Durchprobieren von Passwörtern *https://cwe.mitre.org/data/definitions/307.html*) einstellen
- Service Zugang scheint auf den ersten Blick uninteressant für Angreifer
  - Monitoring Interface
  - Ob man sich als Admin oder User anmeldet macht keinen Unterschied
  - Einstellungen können nicht geändert werden etc.
  - Wahrscheinlich daher keine größen Schutzmaßnahmen wie beim Client Login

5 Finding 2: WinGuard Service Zugang - Passwort Brute Force

Passwort Brute Force

- Jedoch **keine** speziellen Nutzer für den Servicezugang!
- Daher die Idee:

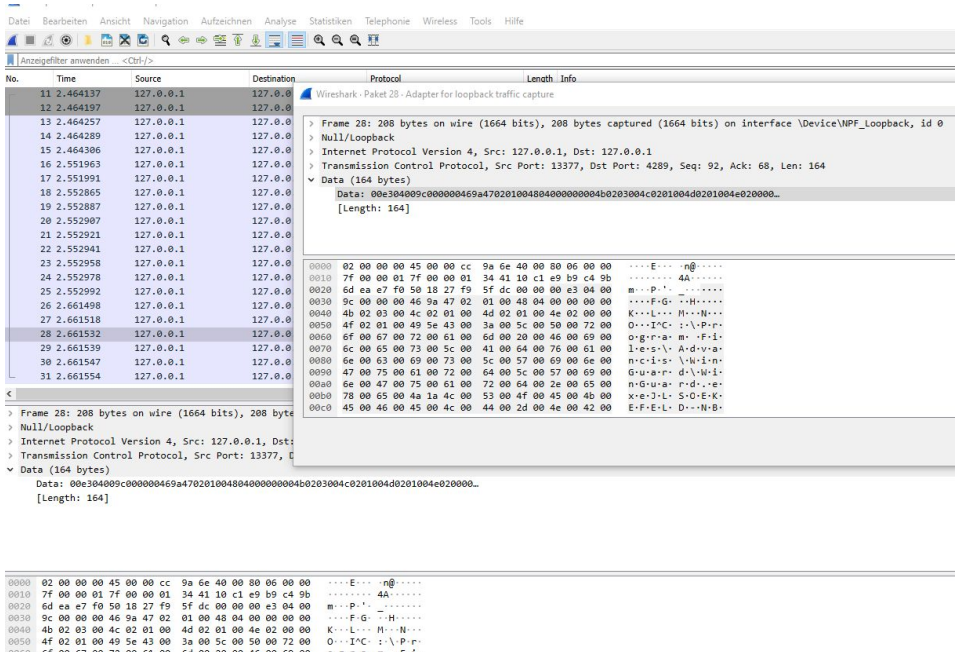
  Brute Force der Passwörter über den Servicezugang

Sicherheitsproblem!
Brute-Force-Schutz greift **nicht** beim Servicezugang!

5 Finding 2: WinGuard Service Zugang - Passwort Brute Force

Winguard Service Zugang - Protokoll

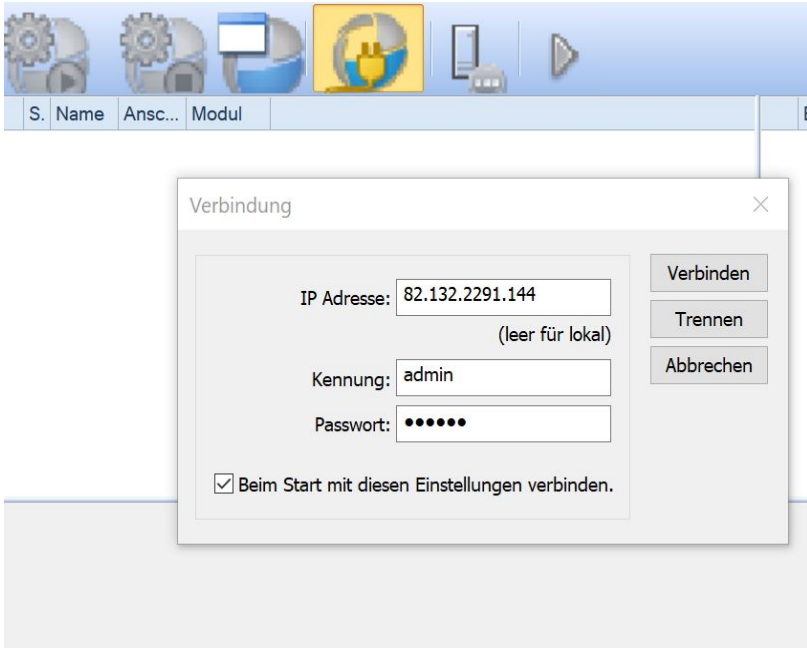
- Der Service Zugang nutzt ein eigenes Protokoll, welches nicht dokumentiert ist
- Bitweise Analyse der übertragenen Daten:
  - Keine Verschlüsselung eingesetzt!
  - Protokoll wurde soweit nachvollzogen, bis ein Login versuch möglich war



5 Finding 2: WinGuard Service Zugang - Passwort Brute Force

Passwort Brute Force

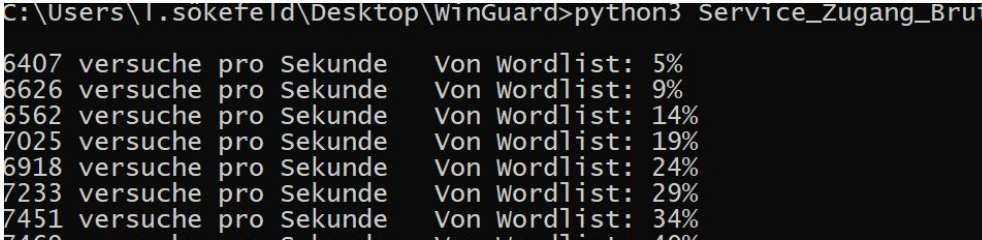
- Fehlende Verschlüsselung ermöglicht es einem Angreifer Passwörter im Netzwerk einfach mitzulesen!
- Die Verschlüsselung lässt sich auch nicht aktivieren (ist nicht vorgesehen, siehe Screenshot der Service Panel Oberfläche)
- Verbreitete Netzwerk Sniffer wie z.B. Wireshark genügen um das Passwort im Klartext zu erhalten!



5 Finding 2: WinGuard Service Zugang - Passwort Brute Force

Passwort Brute Force

- Auf Basis der Protokollanalyse, wurde ein kleines Programm entwickelt, welches Passwörter für einen Benutzer-Account ausprobiert
- Pro Sekunde sind einige tausend Passwort-Versuche möglich
  - Vier Gleichzeitige Verbindungen werden zum Server aufgebaut, je nach Netzwerkverbindung kann diese Zahl noch erhöht werden
  - Abhängig von der Position des Angreifers im Netzwerk
- Wortlisten mit Passwörten können mit bekannten Programmen auf das Ziel zugeschnitten werden
  - crunch
  - cewl



5 Finding 2: WinGuard Service Zugang - User Enumeration

Servicezugang: User Enumeration

Effektives Passwörter raten über den Servicezugang ist nun möglich

Doch was wenn der angegebene Benutzer nicht existiert?

5 Finding 2: WinGuard Service Zugang - User Enumeration

Beobachtung

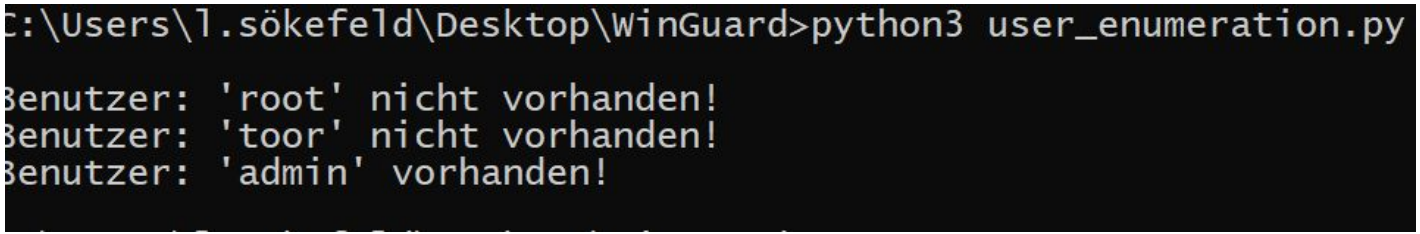
- WinGuard verhält sich unterschiedlich bei Paketen mit gültigen und ungültigem Benutzernamen
- Beispiel:
  - 1. Packet [Benutzer: root , Passwort: dummy] → Antwort: 24 Bytes
  - 2. Packet [Benutzer: toor, Passwort: dummy] → Antwort: 24 Bytes
  - 3. Packet [Benutzer: admin , Passwort: dummy] → Antwort: 1024 Bytes
- Bei gültigem Benutzer (Hier admin) ist die Antwort länger als bei nicht vorhanden Benutzern (root und toor)
- Auf der Winguard Seite scheint Zeit ein Faktor zu sein, daher ist das vorgehen nicht komplett deterministisch
  - Bei Tests mit einigen 100 Benutzernamen gab es jedoch eine Treffsicherheit > 90%

5 Finding 2: WinGuard Service Zugang - User Enumeration

Entwicklung eines Programms zur User enumeration

Programm bekommt Benutzernamen übergeben und prüft ob dieser vorhanden ist

- kann prüfen, ob z.B. der Benutzer: admin existiert
- kann mit einer Wordlist Benutzernamen herausfinden



6 Zusammenfassung

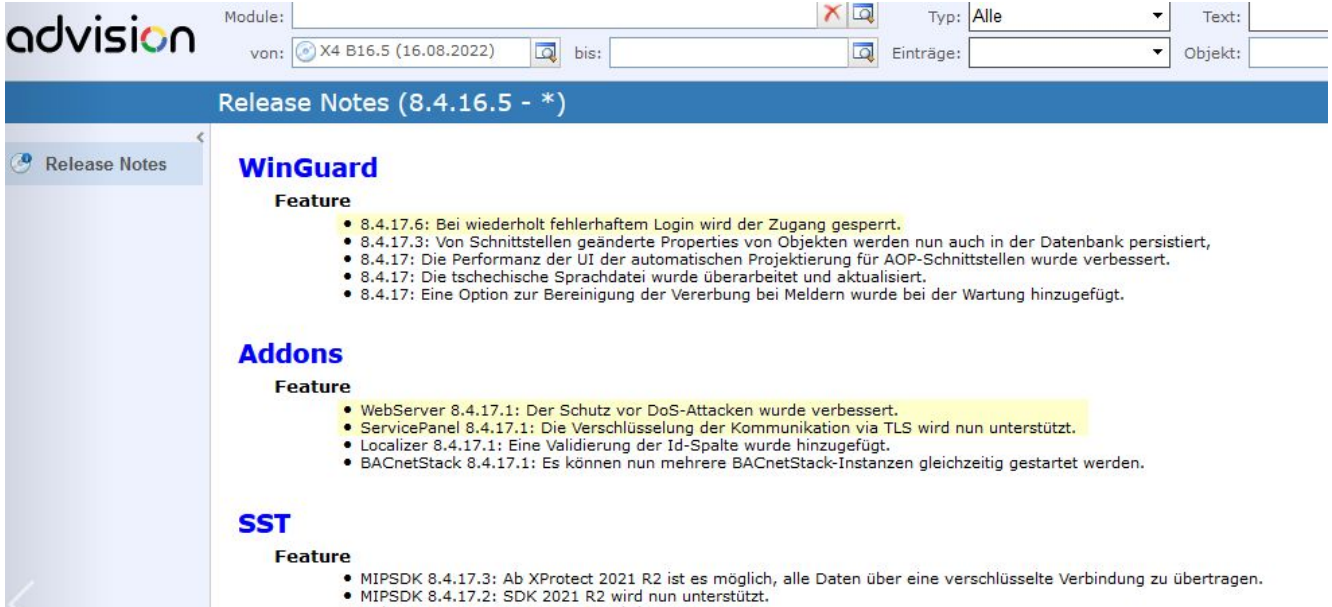
- Die Analyse hat gezeigt, dass für einen Angreifer praxisrelevante Sicherheitslücken in WinGuard gibt.
- Abhängig von der genutzten Konfiguration (Wird der Webserver genutzt? Ist der Service Zugang aktiviert?) lässt sich entweder der Betrieb von WinGuard massiv stören (Denial of Service) oder schlimmer noch der Angreifer kann Login Daten erhalten (Entweder durch mitlesen des Netzwerkverkehrs oder durch ausprobieren).

Als sofortige Reaktion, darauf sollte die aktuell WinGuard Version eingespielt werden

6 Zusammenfassung

Was ist dann passiert?

- Schnelle und professionelle Reaktion des Herstellers
- Behebung der Lücken in der aktuellen Version



Fragen?

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e.V.

CONCEPTURE