RAPID7

23. Oktober 2024

Honeypots

Klebefallen für Angreifer

Andreas Galauner
Lead Security Researcher (Threat Analytics)

Wasn das fürn Typ?

Andreas Galauner

Lead Security Researcher

Labs / Threat Analytics

- Wohnt in Aachen
- Full-time Nerd und Hacker
- Ich mag Computer (und alles was versucht zu verheimlichen, dass es einer ist)
- Ehemaliger CTF-Spieler (berentet…)
- Spezialitäten: IoT, Hardware, Betriebssysteme, alles was relativ weit unten in den Schichten ist
- Seit 9-10 Jahren bei Rapid7, je nachdem wie man zählt

Rapid7 Threat Analytics

Mehrere Betätigungsfelder:

- Emergent Threats
  - Analyse von aktuellen Bedrohungen
  - Content Creation und Analyse für Produkte und Community

- Security Community
  - Metasploit Module
  - AttackerKB

- Internet Scale Data & Research
  - Sonar
  - Doppler
  - Heisenberg (Lorelei)
  - Beehive (aktueller Projektname)

Honeypots

Mit Honig fängt man Fliegen

Wie? Watt? Honeypot?

- Heutige Bedrohungslagen werden schnell komplex:
  - Scriptkiddies die nur ein paar Coins minen wollen
  - Kriminelle Gruppen die per Ransomware Lösegeld erpressen
  - Staatlichen Gruppen die zerstörerischen Einfluss ausüben wollen
  - Hacktivisten die politische Ziele verfolgen
  - Gelangweilte Teenager die Spielequellcode und Trailer klauen
  - ... und ein Mix aus all dem und was ich sonst noch so vergessen habe

Wär ganz gut, wenn wir wüssten was die so tun bevor es einen selbst erwischt…

Also Stellen wir Fallen auf: Honeypots.

Honeypots tun so als seien sie ein verwundbares System und warten auf Angreifer. Dabei wird jede Interaktion zur späteren Auswertung und Aufklärung mitprotokolliert.

Low vs High Interaction

Arten von Honeypots

Low Interaction

Idee:

- Irgendein Protokoll nehmen und selbst einen Server implementieren
- Dabei nur das notwendigste Implementieren um die Infos zu bekommen die man haben will
- … und schön alles mitloggen was abgeht

Vorteile:

- Relativ easy zu bauen
- So schnell bricht da keiner aus, wenn man das nicht will

Nachteile:

- Relativ offensichtlich für Angreifer
- Extrem unflexibel
- Sicherheitslücken müssen ebenfalls nachgebaut werden

High Interaction

Idee:

- Realen (oder virtualisierten) Server nehmen und irgendwo hinstellen
- Von außen aufs Betriebssystem gucken
- … und schön alles mitloggen was abgeht

Vorteile:

- Reale Software, schwer für Angreifer zu erkennen
- Super flexibel, richtige Sicherheitslücken

Nachteile:

- Kompliziert zu bauen
- Ausbrüche möglich

Project Beehive

… oder wie auch immer es mal heißen wird

Beehive

Wir brauchen endlich flexible high interaction honeypots

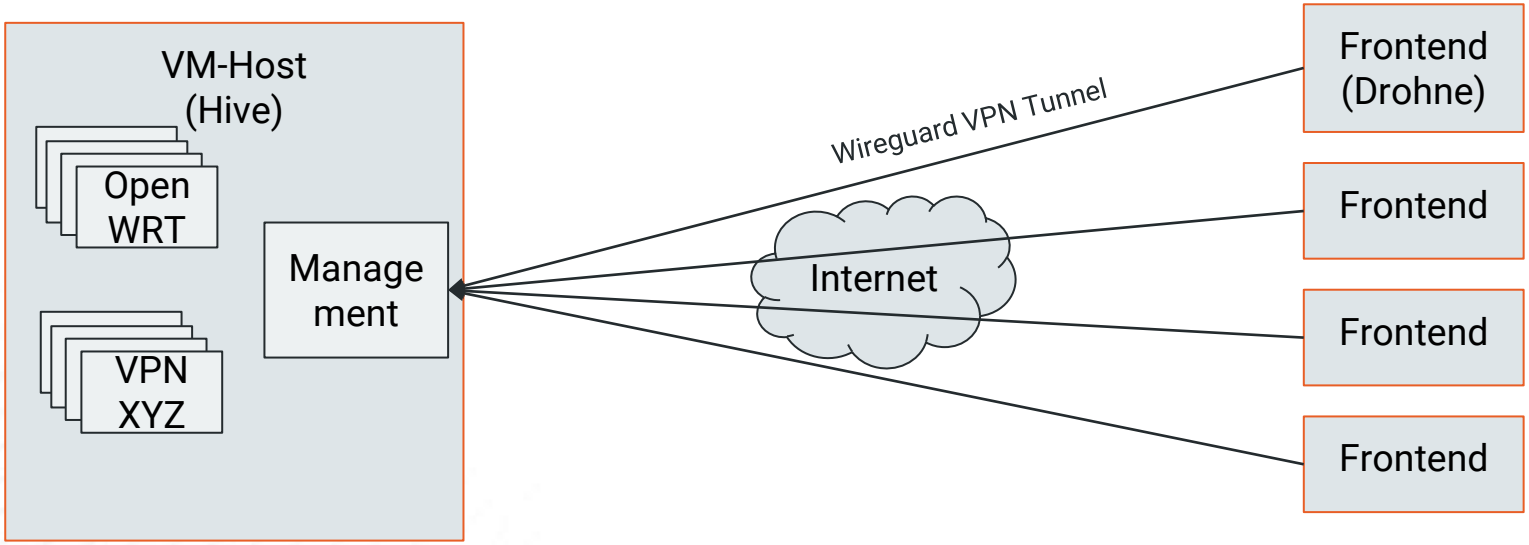
- Deployment von neuen und bisher unbekannten Services muss viel schneller gehen
- Wir können unmöglich alles nachbauen
- Wartungsaufwand sollte möglichst gering sein, weniger als aktuell mit Heisenberg
- Selbst wenn wir wirklich alles nachbauen könnten, würden wir noch immer nicht alle, vor allem unbekannte, Bugs nachbauen können - und die wollen wir ja eigentlich finden

Beispiel:

1. Neuer Bug in VPN appliance XYZ? Was nun?
2. VPN appliance XYZ als Honeypot-VM starten
3. Ins Internet hängen
4. Warten und Angreifer fangen
5. Exploit Analysieren

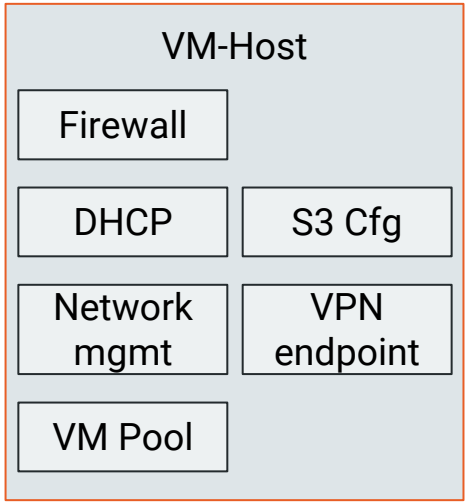
Es führt kein Weg mehr daran vorbei endlich mal welche zu bauen

Beehive


VM-Host
(Hive)
Open
WRT
VPN
XYZ
Manage
ment
Wireguard VPN Tunnel
Internet
Frontend
(Drohne)
Frontend
Frontend
Frontend

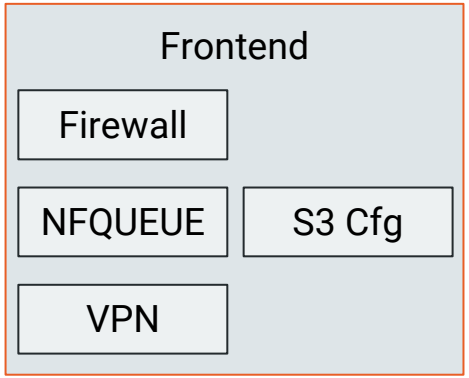
VM-Host (Hive)

- Eine dicke Kiste irgendwo im Rechenzentrum
- Startet, besorgt sich ne Config von irgendwo
- Lädt nen Haufen VMs runter
- Startet sie, wartet bis sie gebootet haben und legt sie auf Halde
- Verwaltet ne Firewall, sodass die VMs möglichst alleine stehen und nicht mit anderen quatschen
  - Verwaltet auch ausgehenden Traffic
  - Routet evtl. über shady VPN, macht rate-limiting etc.
- Verwaltet VPN-Infrastruktur, damit die Drohnen zurück zum Stock finden



Frontend (Drohne)

- Viele kleine VMs irgendwo in Cloud environments
- Startet, besorgt sich ne Config von irgendwo
- Verbindet sich mit dem Bienenstock per VPN
- Konfiguriert seine Firewall um eingehende Verbindungen zu erkennen
  - Für die Linux nerds: nftables und nfqueue
- Drohnen leiten Traffic an Hive für jeden Angreifer
- Angreifer bekommt eigene, isolierte VM als Spielwiese



Junge, warum so kompliziert?

Design hat mehrere Vorteile:

- Frontends sind super klein und brauchen keine CPU-Power
  - Können mehrere Dienste anbieten
- VMs können von anderen Teams selbst erstellt werden
  - Windows
  - Linux
  - Custom OS
- Volle kontrolle über Netzwerktraffic
  - Egress kann über “shady” VPNs gehen
  - Wir können rate-limiten
  - Wir können mitlesen
- Die Dienste sehen 100% echt aus
- Angreifer der sich zweimal verbindet bekommt zweite Connection auf die SELBE VM
  - Unglaublich cooles Feature

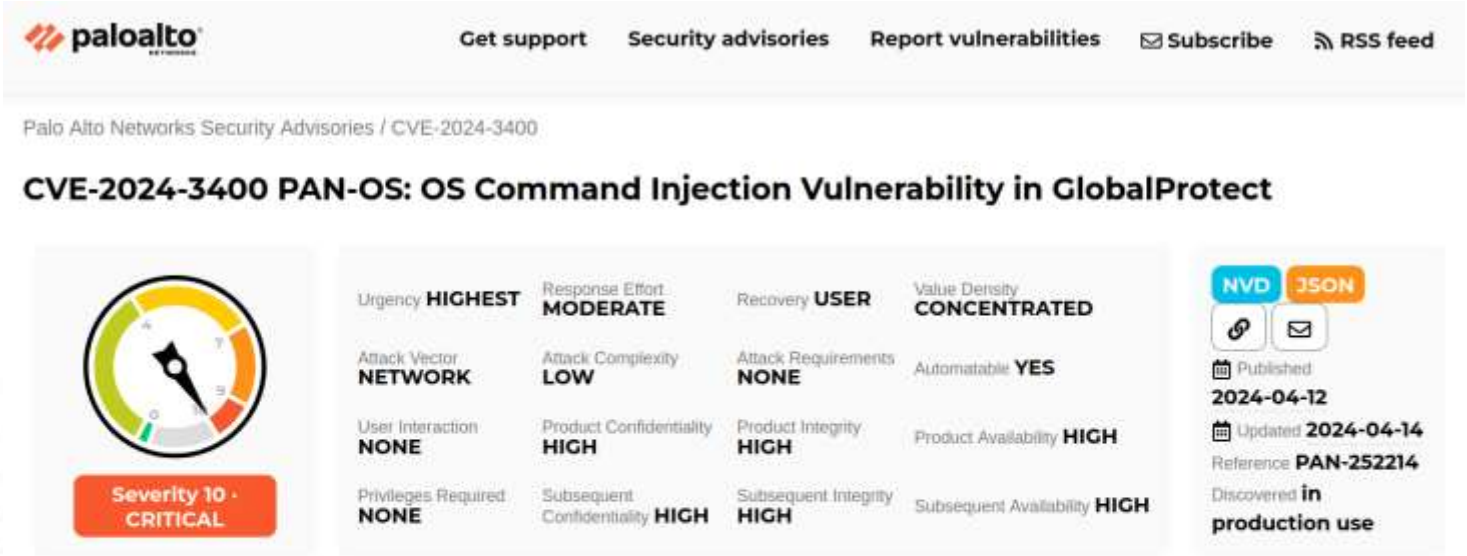
Okay und das funktioniert?

Öhm, naja. Sehr warscheinlich…

Aktueller Status:

- Alles in Rust geschrieben
  - Thread-safe, memory-safe, schnell, ideal für systems programming
  - Die Zukunft!!!1!
- Frontend fertig
  - Connections kommen rein
  - Backend wird bescheid gesagt
  - Firewall wird konfiguriert
- Backend fast fertig
  - VMs werden gestartet
  - VMs werden auf Zuruf reserviert
  - Alles wird wieder aufgeräumt
- Intelligence Gathering
  - Aktuelle Baustelle

Und dann?



paloalto

Get support | Security advisories | Report vulnerabilities | Subscribe | RSS feed

Palo Alto Networks Security Advisories / CVE-2024-3400

CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect

Severity 10 · CRITICAL

Urgency **HIGHEST**	Response Effort **MODERATE**	Recovery **USER**	Value Density **CONCENTRATED**
Attack Vector **NETWORK**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **YES**
User Interaction **NONE**	Product Confidentiality **HIGH**	Product Integrity **HIGH**	Product Availability **HIGH**
Privileges Required **NONE**	Subsequent Confidentiality **HIGH**	Subsequent Integrity **HIGH**	Subsequent Availability **HIGH**

NVD JSON

Published **2024-04-12**

Updated **2024-04-14**

Reference **PAN-252214**

Discovered **in production use**

Description

A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Fixes for PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 are in development and are expected to be released by April 14, 2024. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. All other versions of PAN-OS are also not impacted.

Und dann?

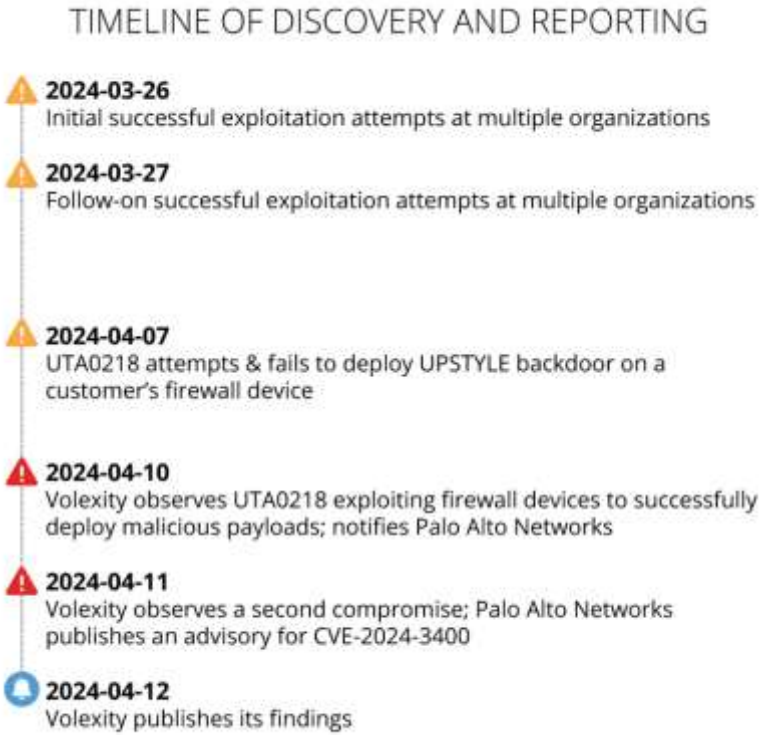
Schön aufn Freitag mal ne Vulnerability droppen

- Base Score von 10.0
- Pre-Authentication
- Remote Code Execution

Richtiges 0-day!

Perfekt um nen Honeypot irgendwo hinzustellen und zu warten bis mal einer vorbeikommt.

Vielleicht (!) irgendwann sogar mal in Kundennetzwerken. Vielleicht! Nur sone Idee! Wirklich nur ne Idee!



Quelle: https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Fertig!

Kommt gerne an unseren Stand! 

Mehr Research: **rapid7.com/research**

E-Mail: **andreas_galauner@rapid7.com**