T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Analyse von Angriffsflächen bei Shared-Hosting-Anbietern

Chris Wojzechowski, 06.11.2024

Motivation

Shared Hosting im Fokus

- Zielgruppe: KMUs
- Risiko besteht in der geteilten Nutzung von Hardware

Unsere Forschung

- 30 zufällig ausgewählter Hoster
- 4319 gefundene Benutzernamen
- Detailanalyse von drei Hostern

Forschungsfragen

- Welche Methoden können für “Privelege Escalation” in der Praxis umgesetzt werden?
- Welche Sicherheitslücken gibt es bei Shared Hosting Anbietern in der Praxis?
- Welche Sicherheitsmaßnahmen werden von den Shared Hosting Anbietern in der Praxis eingesetzt?

Methodik

Angreifer Modell

- Registrierung mit dem Ziel an Daten anderer Kunden zu kommen
- Fokus auf dem Sammeln von CVEs
  - Live-Systeme, daher kein aktives Ausnutzen der Schwachstellen

Anbieter Auswahl

- Um die Reproduzierbarkeit sicherzustellen, wurde die Liste von *Datanyze* verwendet
- Zufällige Auswahl von 30 Anbietern, die eine Verbindung mit SSH erlauben

Methodik

Automatische Analyse

- Ausführen des eigenen Skripts
- Analyse von 13 Schwachstellen und dem Zugriff auf sensible Informationen

Manuelle Analyse

- Herunterladen der vorinstallierten Binaries
- Analyse der installierten Kernel-Version und weiterer Benutzer auf dem System

Ergebnisse

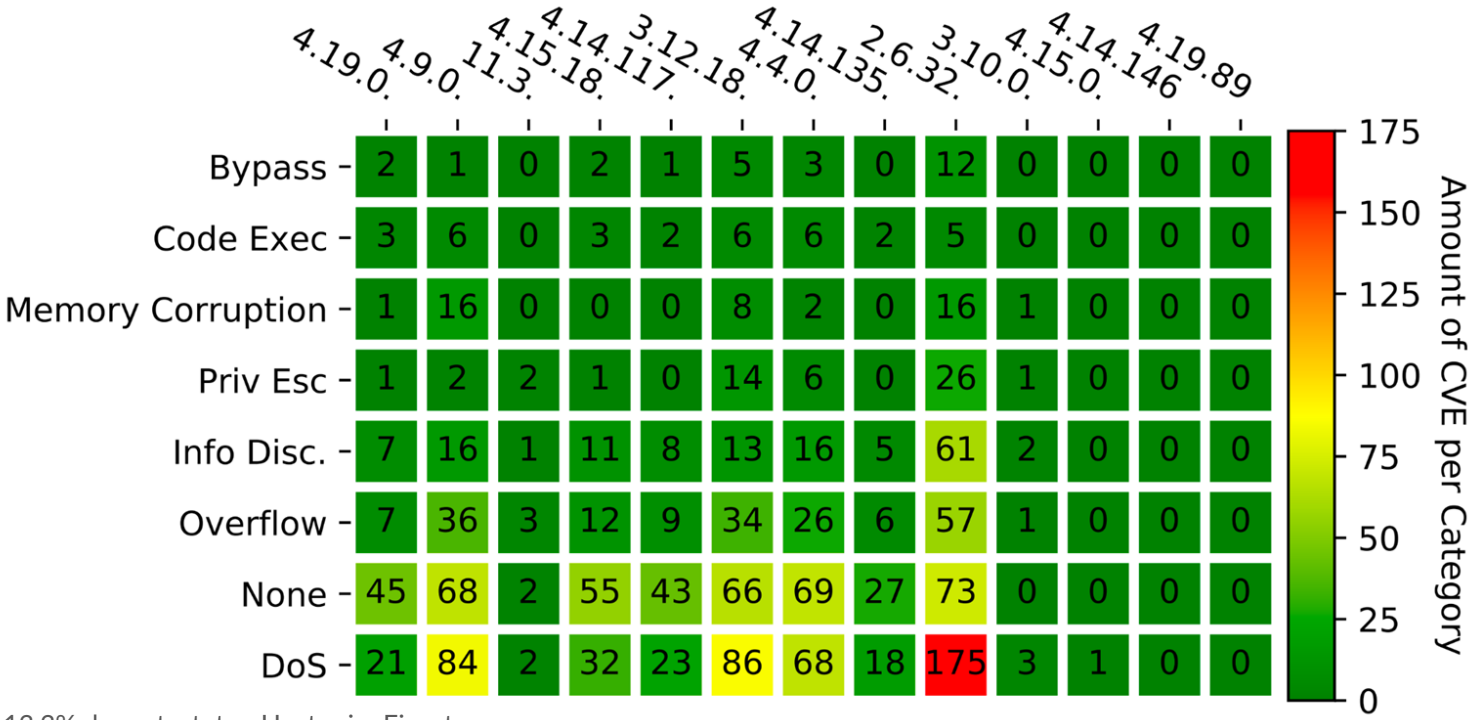
Operating System Security Level

Kernel-Versionen

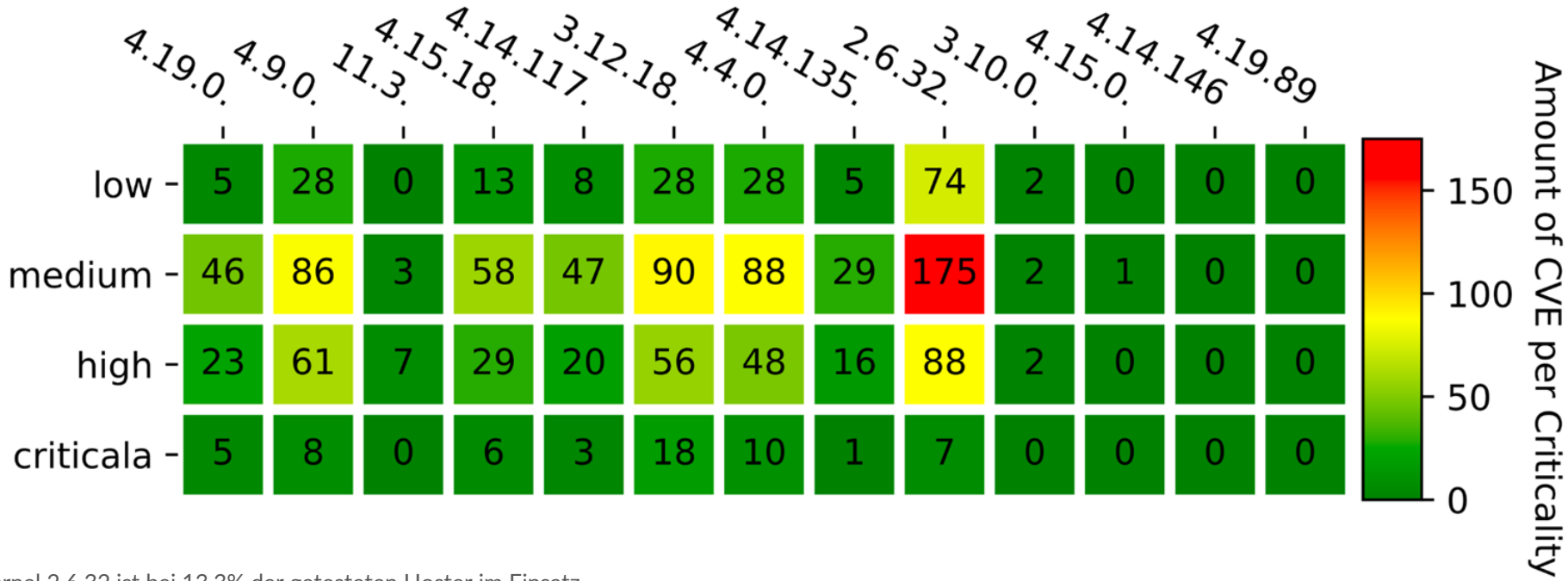
- 13 unterschiedliche Kernel-Versionen im Einsatz
- 83% (25 von 30) der Kernel-Versionen besitzen mind. eine bekannte Sicherheitslücke

Arten der Schwachstellen

- 93,3% der Systeme besitzen Sicherheitslücken, die dem Nutzer root-Rechte geben
- Großteil der Sicherheitslücken schränkt “nur” eins der drei Schutzziele ein



Kernel 2.6.32 ist bei 13,3% der getesteten Hoster im Einsatz



Kernel 2.6.32 ist bei 13,3% der getesteten Hoster im Einsatz

System Specific Findings

- Zwischen 0 und 41 Programme liefen mit dem SUID bit gesetzt
  - Ein Hoster führte ein Program aus, dass dem User das Ausführen einer root shell ermöglicht

- Schreibrechte im /etc/-Ordner bei 13 Anbietern
  - Mail-Server-Einstellungen und Web-Server-Einstellungen können verändert werden

- Unmounted Dateisystem bei einem Anbieter
  - Es ist erfolgreich gewesen ein geteiltes Dateisystem lokal einzubinden, sodass sensible Informationen anderen Nutzer einsehbar gewesen sind

System Specific Findings

- Lese- und Schreibberechtigungen
  - 3 Anbieter erlaubten das Lesen anderer webroots und 1 Anbieter erlaubte das Lesen des gesamten home-Ordners
  - Schreibberechtigungen deutlich konsequenter gesetzt

- Sensible Informationen in Logs
  - 5231 Zeilen von Log-Daten wurden mithilfe von Schlüsselwörtern durchsucht
  - 27% lieferten Ergebnisse die mind. ein Schlüsselwort enthalten haben
  - Fremder Zugriff auf das lokale System, lokale Datenbank, … sind möglich

```
/var/log/cpanel-install.log:[20130625.185616]   /usr/bin/mysqladmin -u root password 'XXXXXXXXXX'
/var/log/cpanel-install.log:[20130625.185616]   /usr/bin/mysqladmin -u root -h XXXXXXXXXX.com password 'XXXXXXXXXX'
```

Manuelle Analyse

- Installierte Software
  - Viele Versionen von Programmen installiert (im Schnitt 7,75 Python-Versionen und 6,25 PHP-Versionen)
  - 22 CVEs konnten für die drei analysierten Anbieter gefunden werden

- Konfigurations-Files
  - Bei allen Anbietern konnte die installierte Version des Kernels, die Distrubution und die System-Architektur herausgefunden werden -> 50 potenzielle Exploits, zwischen 2 und 16 Schwachstellen pro Anbieter

- Nutzer auf dem System
  - Es konnte bei allen Anbietern die passwd-Datei gefunden und gelesen werden
  - Viele Einträge konnte identifiziert werden, dessen Zuordnung sich durch die Namensgebung oder den Speicherort erschließen lässt
    - “uberrroot”
    - /etc/cbi/group/ftpusers

Limitations

- Durch das fehlende Exploiten der gefundenen Schwachstellen, kann der wirkliche Nutzen für Angreifende nicht verifiziert werden.
- Unser intuitiver Ansatz zum Auffinden der Schwachstellen kann nicht als vollständig angesehen werden, sodass es weitere Wege für Angreifende geben kann.
- Die Messung wurde bereits im Jahr 2020 durchgeführt.

Zukünftige Arbeiten

- Registrierung von mehreren Benutzern, um mögliche Datendiebstähle tiefergehend testen zu können.
- Mit den Hosting-Anbietern in Kontakt treten, sodass das Exploiten auf bspw. Test-Systemen erlaubt wird, um die genannte Limitation auszuräumen.

Zusammenfassung

- Privelege Escalation ist eine große Gefahr im Bereich von Shared Hosting Services.
- Der Einsatz veralteter Kernel-Versionen sorgt für das Vorhandensein mehrere teils kritischer Schwachstellen.
- Patch-Management oder strikte Mandantentrennung würde die Sicherheit der getesteten Services signifikant erhöhen.

T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Vielen Dank für Ihre Aufmerksamkeit!

Chris Wojzechowski, 06.11.2024