

Task: Conficker-Suche

Inhalt

- [Suchmethoden für Schwachstellen und Befall](#)
- [Suche nach Schwachstelle und Conficker ausführen](#)

Einleitung

Conficker ist ein im Herbst 2008 aufgetauchter Wurm der Windows Betriebssysteme gefährdet und zu zahlreichen Ausfällen sowie umfangreichen finanziellen Schaden geführt hat. Er nutzt eine Sicherheitslücke des Betriebssystems aus und aktualisiert sich selbst.

Das Microsoft Bulletin [MS08-067](#) beschreibt die wichtigste Sicherheitslücke die Conficker ausnutzt um das betreffende System zu befallen.

Suchmethoden für Schwachstellen und Befall

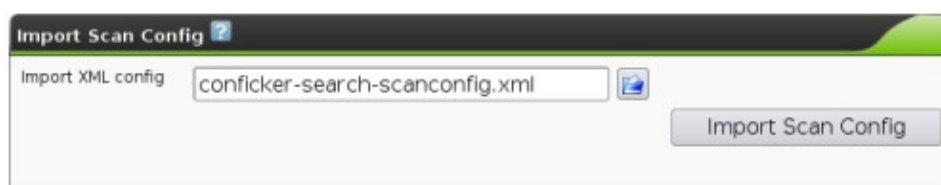
Mit dem Greenbone Security Manager empfehlen sich zwei unterschiedliche Methoden zur Suche:

- Suche nach Systemen, die mit der Conficker infiziert sind, kombiniert mit einer nicht-invasiven Suche nach der von Microsoft im Bulletin MS08-067 beschriebenen Sicherheitslücke.
- Invasive Suche nach der von Microsoft im Bulletin MS08-067 beschriebenen Sicherheitslücke, ebenfalls inklusive der Conficker-Suche.

Die erste Methode kann nicht in allen Fällen das Vorhandensein der Schwachstelle aufdecken. Die zweite Methode geht für das Aufdecken soweit, dass versucht wird die Schwachstelle selbst auszunutzen um Gewissheit zu bekommen ob sie vorliegt. Dabei kann es allerdings zum Ausfall des betreffenden Systems kommen und sollte nur mit entsprechender Umsicht ausgeführt werden.

Suche nach Schwachstelle und Conficker ausführen

1. Importieren Sie die Scan Configuration [Conficker Search](#) oder für die invasive Suche die Scan Configuration [Invasive Conficker Search](#).








2. Falls das Zielsystem keine anonyme Anmeldung erlaubt, erstellen Sie Credentials um der Scan-Engine Zugang zu den Zielsystemen zu geben. Falls noch nicht geschehen, erstellen Sie dafür

einen entsprechenden Anwender auf Ihren Windows-Systemen (ein niedrig privilegiertes Benutzer-Konto reicht aus).

3. Legen Sie die Zielsysteme (Targets) fest und wählen Sie ggf. die entsprechenden Credentials.

4. Nun können Sie die Aufgabe (Task) erstellen. Dafür kombinieren Sie die oben importierte Scan Configuration mit dem entsprechend erstellten Zielsystemen.

5. Die Suche wird gestartet indem Sie für den eben erstellten Task auf  klicken. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.

| Report | Threat | Scan Results | | | | Download | Actions |
|---------------------------------|--------|--------------|--------|-----|-----|--|---|
| | | High | Medium | Low | Log | | |
| Mon Feb 1 10:54:02 2010 Done | High | 1 | 0 | 0 | 4 | PDF  Download |   |

6. Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen. Hier ein Beispiel für ein System bei dem das Hersteller-Update für MS08-67 nicht eingespielt wurde.

Filtered Results

| Host | High | Medium | Low | Log | Total |
|-----------------------------|------|--------|-----|-----|-------|
| 192.168.2.6 | 1 | 0 | 0 | 0 | 1 |
| 192.168.2.9 | 0 | 0 | 0 | 0 | 0 |
| Total: 2 | 1 | 0 | 0 | 0 | 1 |

Port summary for host "192.168.2.6"

| Service (Port) | Threat |
|----------------|--------|
| general/tcp | High |

Security Issues reported for 192.168.2.6

| High | general/tcp |
|---|-------------|
| <p>NVT: Server Service Could Allow Remote Code Execution Vulnerability (958644) (OID: 1.3.6.1.4.1.25623.1.0.900055)</p> <p>MS08-067</p> <p>Overview: This host has critical security update missing according to Microsoft Bulletin MS08-067.</p> <p>Vulnerability Insight: Flaw is due to an error in the Server Service, that does not properly handle specially crafted RPC requests.</p> <p>Impact: Successful exploitation could allow remote attackers to take complete control of an affected system.</p> <p>Variants of Conficker worm are based on the above described vulnerability. More details regarding the worm and means to resolve this can be found at, http://technet.microsoft.com/en-us/security/dd452420.aspx</p> <p>Impact Level: System</p> <p>Affected Software/OS: Microsoft Windows 2K Service Pack 4 and prior. Microsoft Windows XP Service Pack 3 and prior. Microsoft Windows 2003 Service Pack 2 and prior.</p> <p>Fix: Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms08-067.aspx</p> <p>References: http://www.microsoft.com/technet/security/bulletin/ms08-067.aspx</p> <p>CVSS Score: CVSS Base Score : 9.3 (AV:N/AC:M/Au:NR/C:C/I:C/A:C) CVSS Temporal Score : 7.3 Risk factor: High CVE : CVE-2008-4250</p> | |