# Microsoft HTTP.sys Schwachstelle (MS15-034)

| | |
|---|---|
| **Version** | 1.0 |
| **Datum** | 16. April 2015 |
| **Kontakt** | ms15034@sba-research.org |

## Was ist MS15-034?

Microsoft hat im Zuge des Patch-Tuesdays am 14.4.2015 einen Patch für eine als kritisch eingestufte Lücke im Windows HTTP Protokoll Stack (auch bekannt als HTTP.sys) veröffentlicht. Die Lücke wird als kritisch eingestuft, weil sie von einem **externen** Angreifer ausgenutzt werden kann, sofern MS IIS (Internet Information Service) auf dem System ausgeführt wird. Laut der offiziellen Beschreibung von Microsoft im Bulletin MS15-034[1] könnte die Lücke von einem Angreifer möglicherweise auch für die **Ausführung von eigenem Code** verwendet werden (*remote code execution*), was diesem praktisch die **Übernahme von entfernten Rechnern** mit MS IIS erlauben würde.

## Auswirkungen

Es ist einem Angreifer jedenfalls möglich die Lücke für *Denial of Service* Angriffe zu verwenden. Mit Stand 16.4.2015 sind noch keine *remote code execution* Angriffe bekannt, im Zuge derer ein Angreifer eigene Kommandos auf dem verwundbaren Webserver ausführen und somit den Webserver übernehmen konnte. Viele Sicherheitsforscher vermuten jedoch, dass es nur eine Frage der Zeit ist bis *remote code execution* Angriffe entwickelt werden.

## Betroffene Systeme

Von der Schwachstelle betroffen sind Windows 7, Windows Server 2008 R2, Windows 8 und 8.1, Windows Server 2012 und 2012 R2 Systeme. Nicht betroffen sind Windows Server 2003 Systeme.

In Österreich sind laut der Computersuchmaschine Shodan rund 22.000 Rechner betroffen.

## Überprüfung

Folgender Aufruf des Programms curl ermöglicht es von extern zu prüfen, ob der eigene IIS von der Lücke betroffen ist. Dazu geben Sie folgende Zeile in der Shell ein:

```
curl -v [ipaddress]/ -H "Host: test" -H "Range: bytes=0-18446744073709551615"
```

[1] https://technet.microsoft.com/library/security/MS15-034

Wenn der Server mit „Requested Header Range Not Satisfiable“ antwortet, ist man möglicherweise verwundbar. Da die http Antworten des Servers variieren können, bietet dieser Test allerdings keine hundertprozentige Sicherheit. Es wird daher empfohlen, den Patch auch einzuspielen, wenn manuelle oder automatisierte Scans ein negatives Ergebnis liefern.

## Behebung

Die Schwachstelle wird durch einen von Microsoft am 14.4.2015 veröffentlichten Patch behoben. Die Schwachstelle war vor der Veröffentlichung der Schwachstelle nicht öffentlich bekannt.

Aufgrund der Kritikalität der Schwachstelle **empfehlen wird den von MS veröffentlichten Patch dringend einzuspielen!**

## Kontakt

Für nähere Informationen oder Unterstützung bei der Überprüfung wenden Sie sich bitte an:

ms15034@sba-research.org

SBA Research gGmbH
www.sba-research.org