BOLETÍN DE ALERTA

Boletín Nro.: 2015-04
Fecha de publicación: 15/04/2015
Tema: Ejecución Remota a través de peticiones HTTP en Windows (MS15-034)

Sistemas afectados:
Todas las ediciones compatibles con Microsoft Windows 7, Windows Server 2008 R2, Windows 8, Windows 8.1, Windows Server 2012 y Windows Server 2012 R2.
En esta lista no se incluyen las versiones de Windows cuyo ciclo de vida ha terminado (versiones anteriores a Windows 7), las cuales podrían también ser vulnerables.

Descripción:
Se ha descubierto una vulnerabilidad crítica en la pila de protocolo HTTP (HTTP.sys) de Windows, la cual podría permitir a un atacante la ejecución remota de código arbitrario o causar una denegación de servicio.
La vulnerabilidad se da en el la forma en la que HTTP.sys analiza de forma incorrecta ciertas solicitudes HTTP especialmente diseñadas.
La explotación de dicha vulnerabilidad es extremadamente sencilla, puede ser ejecutada con una sola petición HTTP de forma remota, razón por la cual la vulnerabilidad ha sido calificada como crítica con una puntuación de 10 en la escala CVSS. La vulnerabilidad es especialmente crítica en sistemas con Microsoft IIS.
Ya se han observado diversos exploits disponibles en Internet.

Impacto:
Un atacante que aprovechara esta vulnerabilidad podría ejecutar código arbitrario en el contexto de la cuenta del sistema, así como también causar una denegación de servicio.

Detección:
Se ha publicado un script para la herramienta Nmap que puede ser de utilidad para detectar equipos vulnerables en su red, el cual se encuentra disponible aquí:
https://github.com/cldrn/nmap/blob/master/scripts/http-vuln-cve2015-1635.nse

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Para realizar la prueba, se puede ejecutar:
nmap -p80 --script http-vuln-cve2015-1635.nse <rango de IP de destino>

En caso de encontrar un equipo vulnerable en su red y que tenga el puerto 80 abierto, obtendrá el siguiente resultado:

```
-- PORT   STATE SERVICE REASON
-- 80/tcp open  httpsyn-ack
-- | http-vuln-cve2015-1635:
-- |   VULNERABLE:
-- |   Remote Code Execution in HTTP.sys (MS15-034)
-- |         State: VULNERABLE (Exploitable)
-- |         IDs:  CVE:CVE-2015-1635
-- |         A remote code execution vulnerability exists in the HTTP protocol stack (HTTP.sys) that is
-- |         caused when HTTP.sys improperly parses specially crafted HTTP requests. An attacker who
-- |         successfully exploited this vulnerability could execute arbitrary code in the context of the System account.
-- |
-- |         Disclosure date: 2015-04-14
-- |         References:
-- |         https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
-- |_        http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635
```

Solución:

De acuerdo al boletín MS15-034, Microsoft ha publicado un parche que corrige la vulnerabilidad. El mismo se encuentra disponible desde el Centro de Actualización de Windows (Windows Update) o puede ser descargado de manera manual desde:
https://technet.microsoft.com/en-us/library/security/ms15-034.aspx

Información adicional:

https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635
https://github.com/cldrn/nmap/blob/master/scripts/http-vuln-cve2015-1635.nse
https://ma.ttias.be/remote-code-execution-via-http-request-in-iis-on-windows

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py