

GUÍA TÉCNICA PRÁCTICAS INSTRUCTOR

MÓDULO 7. TALLER 2

TALLER 2: CLASIFICACIÓN CVSS

Clasifique de acuerdo con el CVSS (<https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?calculator&adv&.0>) : en la pasada investigación forense se encontró que el ataque se desarrolló a través de una vulnerabilidad desconocida que le permitió al atacante modificar la información de varios dispositivos desde una ubicación en Argelia y espiar a los dueños de los equipos, se logró identificar que el ataque se dirigía al servicio SMB de sistemas Windows y se transmitía sola a través de la red local e internet, también está en la capacidad de escalar privilegios. Actualmente existe un exploit el cual al ser ejecutado puede generar una Shell reversa y modificar o borrar la información de la máquina víctima.

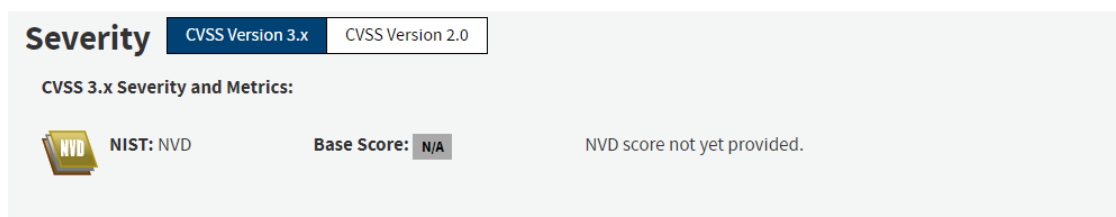
No requiere de autenticación, con la ejecución del exploit, la remediación es oficial por parte de la casa desarrolladora y también tiene un informe de confianza. Solo se permite una sesión del Shell reverso por ataque, no varias sesiones simultaneas.

CVE-2014-8109

DESCRIPCIÓN.


mod_lua.c en el módulo mod_lua en el Servidor HTTP Apache 2.3.x y 2.4.x hasta 2.4.10 no soporta una configuración httpd en la que el mismo proveedor de autorización Lua es usado con diferentes argumentos dentro de diferentes contextos, lo que permite a atacantes remotos saltarse las restricciones de acceso previstas en circunstancias oportunistas aprovechando múltiples directivas Require.

INFORMACIÓN.



Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD** **Base Score:** N/A **NVD score not yet provided.**

En la versión 3.x aún no ha sido reconocida su severidad.

En la versión 2.0 sí tenemos información:

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

 **NIST:** NVD

Base Score: 4.3 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

BASE SCORE DE 4.3 (MEDIUM)

El vector de ataque es a través de la red, con un complejidad de acceso medio sin necesidad de autenticación. Además, no tiene ni impacto en la confidencialidad ni en la disponibilidad, pero sí cierto impacto a nivel de integridad.