UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-006

Actividad Maliciosa Asociada con el Exploit de Internet Explorer Aurora

---

Actividad maliciosa detectada a mediados de diciembre fue dirigida hacia al menos 20 organizaciones de múltiples industrias incluyendo la química, financiera, tecnologías de la información, y medios. Investigaciones acerca de esta actividad revelaron que terceras partes accedieron rutinariamente a cuentas de correo electrónico personales de docenas de usuarios establecidos en Estados Unidos, China y Europa. Futuros análisis revelaron que estos usuarios fueron víctimas de ataques de phishing-scam, por medio de los cuales los actores de amenaza lograron el acceso exitoso a sus cuentas de correo electrónico.

Fecha de Liberación: 25 de Febrero de 2010

Ultima Revisión: 10 de Marzo de 2010

Fuente: US-CERT

Problema de Vulnerabilidad

Local

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

- Microsoft Internet Explorer 6 Service Pack 1 sobre Microsoft Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6, 7, and 8 sobre ediciones sportadas de Windows XP, Windows Server 2003, Windows Vista, Windows 2008,

  Windows 7, y Windows Server 2008 R2

II. Descripción

A través del análisis del código malicioso usando en el incidente, McAfee descubrió que una de las muestras del código malicioso explotó una vulnerabilidad sobre Microsoft Internet Explorer (IE). La vulnerabilidad se manifiesta como una referencia de puntero inválida dentro de IE y, si es explotada satisfactoriamente, permite la ejecución remota de código.

Microsoft ha liberado el Boletín de Seguridad MS10-002, el cual brinda actualizaciones para Internet Explorer que apuntan a esta y otras vulnerabilidades.

El US-CERT está proporcionando indicadores técnicos que pueden ser incorporados dentro del perfil de seguridad de las organizaciones para detectar y mitigar cualquier actividad maliciosa.

Por favor ver https://www.us-cert.gov/cas/techalerts/TA10-055A.html para futuros detalles.

Las siguientes firmas pueden ser desplegadas para asistir in la detección de actividad maliciosa asociada con este incidente:

Alerta de malware primaria

alert tcp any any -> any any (msg:"Targeted Malware Communication Beacon Detected"; flow:to_server,established; dsize:20; content:"|ff ff ff ff ff ff 00 00 fe ff ff ff ff ff ff ff ff ff 88 ff|"; depth:20; sid:7777777; rev:1;)

Alerta de malware secundaria

alert tcp any any any any (msg:"ORC:DIS:BEACON_380DFF"; content:"|38 0d ff 0a d7 ee 9d d7 ec 59 13 56|"; sid:99980060; rev:1;)

Nota: el US-CERT no ha verificado o probado estas firmas y recomienda una apropiada prueba previamente a su utilización.

III. Impacto

Por medio de convencer al usuario de ver un documento HTML tratado especialmente o un documento de Microsoft Office, un atacante puede ser capaz de ejecutar código arbitrario con privilegios del usuario.

IV. Solución

La vulnerabilidad de Internet Explorer usada en estos ataques es tratada con las actualizaciones proporcionadas en el Boletín de Seguridad de Microsoft MS10-002.

Otras recomendaciones incluyen:

- Como una mejor práctica, limitar los permisos del usuario final sobre los sistemas concediendo los derechos administrativos mínimos.
- Activar la Preveción de Ejecución de Datos (Data Execution Prevention, DEP) para IE 6 Service Pack 2 o IE 7. IE 8 activa DEP automáticamente.
- Inspeccionar el historial tráfico de red de las comunicaciones con sistemas externos asociados con el ataque.
- Examinar las computadoras en archivos específicos o atributos de archivo relacionados con el ataque.

V. Referencias

- How Can I Tell if I Was Infected By Aurora? - http://www.mcafee.com/us/local_content/reports/how_can_u_tell.pdf
- How do I know if my organization has been infected? - http://www.mcafee.com/us/threat_center/aurora_enterprise.html
- McAfee Labs Tools Aurora Stinger 10.0.1.765 - http://download.nai.com/products/mcafee-avert/aurora_stinger.exe
- Operation Aurora Hit Google, Others - http://siblog.mcafee.com/cto/operation-%25E2%2580%259Caurora%25E2%2580%259D-hit-google-

- Vulnerability in Internet Explorer Could Allow Remote Code Execution - http://www.microsoft.com/technet/security/advisory/979352.mspx
- Microsoft Security Bulletin MS10-002 - http://www.microsoft.com/technet/security/bulletin/ms10-002.mspx

---

El Departamento de Seguridad en Cómputo/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Jorge Christian Durán Lara (jduran at seguridad dot unam dot mx)
- David Jiménez Domínguez (djimenez at correo dot seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47