UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−027

Actualizaciones de Adobe para Vulnerabilidad en URI de Microsoft Windows

---

Adobe ha liberado actualizaciones para Adobe Reader y la familia de productos de Adobe Acrobat. La actualización soluciona una vulnerabilidad en el manejo de URI en sistemas Microsoft Windows XP y Server 2003 con Internet Explorer 7.

Fecha de Liberación:	24 de Octubre de 2007
Ultima Revisión:	25 de Octubre de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Sistemas afectados**

Los sistemas Microsoft Windows XP y Windows Server 2003 con Internet Explorer 7 y cualquiera de los siguientes productos de Adobe:

- Adobe Reader 8.1 y anteriores
- Adobe Acrobat Professional, 3D, y Standard 8.1 y anteriores
- Adobe Reader 7.0.9 y anteriores
- Adobe Acrobat Professional, 3D, Standard, y Elements 7.0.9 y anteriores

II. Descripción

Las instalaciones de Microsoft Internet Explorer (IE) 7 en Windows XP o Server 2003 cambia la forma en que Windows maneja los llamados URIs (Uniform Resource Identifiers). Este cambio ha introducido una falla que puede causar que Windows determine incorrectamente el manejador apropiado para el protocolo especificado en un URI. Creando un URI de forma específica en un documento PDF, un intruso puede ejecutar comandos arbitrarios en un sistema vulnerable. Más información sobre esta vulnerabilidad en la Nota de Vulnerabilidad del US−CERT VU#403150.

Reportes públicos indican que esta vulnerabilidad está siendo explotada activamente con archivos PDF maliciosos. Adobe ha liberado Adobe Reader 8.1.1 y Adobe Acrobat 8.1.1, los cuales mitigan esta vulnerabilidad.

III. Impacto

Convenciendo a un usuario de que abra un archivo PDF creado de forma específica, un atacante remoto no autenticado podría ser capaz de ejecutar comandos de su elección.

IV. Solución

Aplicar una actualización

Adobe ha liberado Adobe Reader 8.1.1 y Adobe Acrobat 8.1.1 para solucionar este problema. Estos productos de Adobe manejan URIs en una forma que mitiga la vulnerabilidad en Microsoft Windows.

Deshabilitar el URI mailto: en Adobe Reader y Adobe Acrobat

Si es incapaz de instalar y actualizar la versión del software, esta vulnerabilidad puede ser mitigada deshabilitando el manejador del URI mailto: en Adobe Reader and Adobe Acrobat. Consulte el Boletín de Seguridad de Acrobat APSB07−18 para más detalles.

V. Apéndice A. Información del distribuidor

Adobe

Para mayor información sobre la actualización de los productos Adobe afectados, consulte el Boletín de Seguridad de Adobe APSB07−18.

VI. Apéndice B. Referencias

- Boletín de Seguridad de Adobe APSB07−18 − <http://www.adobe.com/support/security/bulletins/apsb07−18.htm>
- Aviso de Seguridad de Microsoft (943521) − <http://www.microsoft.com/technet/security/advisory/943521.mspx>
- Nota de Vulnerabilidad del US−CERT VU#403150 − <http://www.kb.cert.org/vuls/id/403150>

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

- Jesús Ramón Jiménez Rojas (jrojas at 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 43