**UNAM-CERT**

**Departamento de Seguridad en Cómputo**

**DGSCA-UNAM**

---

# Boletin de Seguridad UNAM-CERT-2009-020

## Actualizaciones de Microsoft para múltiples vulnerabilidades

---

Microsoft ha publicado actualizaciones para hacer frente a vulnerabilidades en Microsoft Windows, Windows Server, Componentes de Office Web y Conexión a escritorio remoto para Mac.

| | |
|---|---|
| **Fecha de Liberación**: | 12 de Agosto de 2009 |
| **Ultima Revisión**: | 3 de Septiembre de 2009 |
| **Fuente**: | US-CERT |
| **CVE ID**: | **TA09-223A** |

### Sistemas Afectados

| | | | |
|---|---|---|---|
| **Microsoft Windows** | **Microsoft Office** | **==** | . |
| **Microsoft Windows** | **Microsoft Windows and Windows Server** | **==** | . |
| **Microsoft Windows** | **Remote Desktop Connection Client for Mac 2.0** | **==** | . |

### Riesgo

Crítico

### Problema de Vulnerabilidad

Remoto

### I. Descripción

Microsoft ha publicado múltiples boletines de seguridad para vulnerabilidades criticas en Windows, Windows Server, Componentes Office Web y Conexión a Escritorio remoto para Mac. Estos boletines son descritos en el Boletin de Seguridad de Microsoft para el mes de agosto de 2009.

El boletín de seguridad de Microsoft MS09-037 incluye actualizaciones para componentes de Microsoft para hacer frente alas vulnerabilidades en el Active Template Library (ATL). Las vulnerabilidades presentes en el ATL que puede causar vulnerabilidades como resultado en los controles ActiveX y componentes COM. En el control ActiveX o cualquier Componente de COM que se creo con una version vulnerable de ATL pueden ser vulnerables, intuyendo una distribución por los desarrolladores terceros.

Los desarrolladores deben actualizar el ATL como se describe en la previa publicación del Boletin de seguridad de Microsoft MS09-35 para poner fin a la creación de controles vulnerables. Para hacer frentes alas vulnerabilidades en los controles existentes, recopilar los controles utilizando la version actualizada de ATL. Un nuevo debate acerca de las vulnerabilidades de ATL puede ser encontrada en el Microsoft Security Advisoty 973882.

## II. Impacto

Un atacante podría ejecutar código arbitrario en algunos casos sin interacción del usuario.

## III. Solución

El aplicar actualizaciones de Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en el Boletín de resumen de seguridad de Microsoft para el mes de agosto de 2009. El boletín de seguridad describe los problemas conocidos y relacionados con las actualizaciones.

Se alienta a los administradores tomar nota de estas cuestiones y pruebas de los posibles efectos adversos. Administradores deben considerar la utilización de un sistema de distribución de actualizaciones automáticas tales como Windows Server Update Services (WSUS).

## IV. Referencias


1. * Microsoft Security Bulletin Summary for August 2009 - http://www.microsoft.com/technet/security/bulletin/ms09-aug.mspx
2. Microsoft Security Advisory 973882 - http://www.microsoft.com/technet/security/advisory/973882.mspx
3. Microsoft Update - https://www.update.microsoft.com/microsoftupdate/
4. Windows Server Update Services http://www.microsoft.com/windowsserversystem/updateservices/default.mspx


---

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

- Mayra Villeda (mvilleda at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez 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 47**