

WMF FAQ

Übersetzung des Textes vom Internet Storm Center

Original zu finden unter <http://isc.sans.org/diary.php?storyid=994>

Stand 03.01.2006, Version 1.4

[Am 05. Januar 2006 hat Microsoft, außerhalb des üblichen Patchday-Zyklus' und früher als ursprünglich angekündigt, ein Update für Windows 2000 SP4, Windows XP (SP1 und SP2) und Windows Server 2003 (mit und ohne SP1) veröffentlicht, das die Sicherheitslücke beheben soll: [KB912919 \(MS06-001\)](#). Dieses Update steht seither für diese Windows-Versionen über die [Windows Update-Seite](#) zum Download und zur Installation zu bereit. Diese Übersetzung der WMF-FAQ vom Internet Storm Center wird daher ab sofort nicht mehr aktualisiert!

Benutzer von Windows 98, 98SE und Millenium Edition (Me), finden [hier](#) einen bislang nicht vom ISC eingehend getesteten, aber nach Userberichten funktionieren, inoffiziellen Patch.]

- **Warum ist das Problem so gravierend?**

Die WMF-Sicherheitslücke verwendet Bilder (WMF-Bilder) um beliebigen Code auszuführen. Der Code wird schon beim Betrachten eines Bildes ausgeführt. In den meisten Fällen muss noch nicht einmal etwas angeklickt werden. Selbst Bilder, die auf Ihrem System gespeichert wurden, können den Schadcode ausführen, wenn sie von einer Index-Software indiziert werden. Auch das Betrachten eines Ordners im Windows Explorer in der „Miniaturansicht“, kann den Schadcode zur Ausführung bringen. Microsoft hat angekündigt, den eigenen, offiziellen Patch nicht vor dem 10. Januar 2006 (dem nächsten regulären „Patch-Day“) zu veröffentlichen.

- **Ist es besser Firefox oder den Internet Explorer zu verwenden?**

Der Internet Explorer zeigt das Bild an und führt den Schadcode ohne Warnung aus. Neue Versionen von Firefox fragen Sie vor dem Öffnen des Bildes. Wie auch immer, in den meisten Umgebungen bietet dies nur geringen Schutz, da es sich um Bilder handelt und diese daher als „sicher“ angesehen werden.

- **Welche Windows-Versionen sind betroffen?**

Alle. Windows 2000, Windows XP, (SP1 und SP2), Windows 2003. Alle sind in gewisser Weise betroffen. Mac OS-X, Unix oder BSD sind nicht anfällig.

Hinweis: Falls Sie noch immer Windows 98/Me verwenden, ist dies ein Wendepunkt: wir glauben (ungetestet), dass Ihr System anfällig ist und es keinen Patch von MS geben wird. Ihre Möglichkeiten, das Problem zu entschärfen, sind sehr begrenzt. Sie werden upgraden müssen.

- **Wie kann ich mich selbst schützen?**

1. Microsoft hat bislang keinen Patch veröffentlicht. Ein inoffizieller Patch wurde von Ilfak Guilfanov zur Verfügung gestellt. Unser Tom Liston hat diesen Patch untersucht und wir haben ihn getestet. Die untersuchte und getestete Version, steht unter http://handlers.sans.org/tliston/wmffix_hexblog14.exe bereit (jetzt in Version 1.4, MD5: 15f0a36ea33f39c1bcf5a98e51d4f4f6), PGP-Signatur (mit dem ISC-Schlüssel signiert) unter http://handlers.sans.org/tliston/wmffix_hexblog14.exe.asc.

DANK an Ilfak Guilfanov für die Entwicklung des Patches!

2. Sie können die zugehörige DLL deregistrieren.
3. Virens Scanner bieten einen gewissen Schutz.

Um die DLL zu deregistrieren:

- Klicken Sie „Start“, dann „Ausführen“, geben Sie `„regsvr32 -u %windir%\system32\shimgvw.dll“` (ohne Anführungszeichen) ein und klicken Sie auf „OK“.
- Es erscheint ein Dialogfenster zur Bestätigung, dass die Deregistrierung erfolgreich war. Klicken Sie „OK“ um dieses Dialogfenster zu schließen.

Unsere aktuelle, praxisgerechte Empfehlung ist, beides zu tun, also die DLL zu deregistrieren und den inoffiziellen Patch zu verwenden.

- **Wie arbeitet der inoffizielle Patch?**

Die wmfhotfix.dll wird über die user32.dll in jeden Prozess geladen. Die DLL patcht dann (im Arbeitsspeicher) die gdi32.dll-Funktion „Escape()“, so dass alle Aufrufe über den SETABORTPROC (z.B. 0x09)-Parameter ignoriert werden. Dies sollte Windows-Programmen ermöglichen, WMF-Dateien anzuzeigen und gleichzeitig die Ausführung des Schadcodes verhindern. Die hier zu findende Version des Patches wurde sorgfältig auch im Quellcode überprüft und mit allen bekannten Versionen des Schadcodes getestet. Er sollte unter Windows XP (SP1 und SP2) und Windows 2000 funktionieren.

- **Schützt mich das Deregistrieren der DLL (ohne den inoffiziellen Patch zu installieren)?**

Es kann helfen. Aber es ist nicht narrensicher. Um es klar zu sagen: wir haben einige sehr deutliche Hinweise, dass das einfache Deregistrieren der shimgvw.dll nicht immer erfolgreich ist. Die DLL kann über bösartige Prozessaufrufe, oder die Installation anderer Programme re-registriert werden. Ferner könnte es zu Problemen kommen, wenn die DLL auf einem System re-registriert wird, das den Schadcode beinhaltet aber erst mit der Re-Registrierung der DLL erfolgreich ausführt. Weiterhin könnten andere Möglichkeiten bestehen, die ESACAPE()-Funktion der gdi32.dll zu missbrauchen. Bis ein Patch von MS zur Verfügung gestellt wird, empfehlen wir die Anwendung des inoffiziellen Patches zusätzlich zur Deregistrierung der shimgvw.dll.

- **Sollte ich die DLL einfach löschen?**

Möglicherweise keine schlechte Idee, aber der Windows-Dateischutz (Windows File Protection) wird sie möglicherweise wieder ersetzen. Sie müssten den Windows-Dateischutz zuerst deaktivieren. Ferner müssten Sie die DLL wiederherstellen, wenn Microsoft einen offiziellen Patch zur Verfügung stellt (Umbenennen anstatt Löschen ist möglicherweise besser, so dass die Datei im Bedarfsfall greifbar ist).

- **Sollte ich nicht einfach alle .WMF-Bilder abblocken?**

Das könnte helfen, ist aber nicht ausreichend. WMF-Dateien werden über einen speziellen Header erkannt, also unabhängig der Dateierweiterung. Die Dateien könnten jede beliebige Dateierweiterung tragen oder in Word- oder anderen Dokumenten eingebettet sein.

- **Was ist DEP (Data Execution Protection / Dateiausführungsverhinderung) und wie hilft es mir?**

DEP wurde von Microsoft mit Windows XP SP2 eingeführt. Es schützt gegen ein breite Palette von Schadcode, in dem es die Ausführung von „Daten Segmenten“ verhindert. Aber, um gut zu funktionieren, erfordert DEP Hardware-Unterstützung. Manche Prozessoren (CPUs) wie z.B. 64 Bit Prozessoren von AMD, bieten volle DEP-Unterstützung und verhindern die Ausführung des Schadcodes.

- **Wie gut wirken Antiviren-Produkte gegen den Schadcode?**

Momentan sind uns Versionen des Schadcodes bekannt, die nicht von Virenscannern erkannt werden. Wir hoffen, dass sie dies bald können. Aber es wird ein harter Kampf, um alle Versionen des Schadcodes erkennen zu können. Aktuell gehaltene Virenscanner sind notwendig, aber wahrscheinlich nicht ausreichend.

- **Wie kommt eine bösartige WMF-Datei auf meinen Rechner?**

Es gibt zu viele Möglichkeiten, als dass man sie alle nennen könnte. E-Mail-Dateianlagen, Web-Seiten und Instant Messaging (Kurznachrichten) sind die wahrscheinlichsten Quellen. Nicht zu vergessen P2P-File-Sharing (Tauschbörsen) und andere Quellen.

- **Ist es ausreichend, Anwendern den Besuch nicht vertrauenswürdiger Web-Seiten zu untersagen?**

Nein. Es hilft, aber es ist nicht ausreichend. Wir hatten zumindest eine, weithin als vertrauenswürdige angesehene Web-Site (knoppix-std.org), die kompromittiert wurde. Als Teil des Hacks wurde ein Frame in die Seite eingebaut, der Besucher zu einer bösartigen WMF-Datei umleitete. „Vertrauenswürdige“ Seiten wurden auch schon in der Vergangenheit gehackt.

- **Was ist das aktuelle Problem mit WMF-Bildern?**

WMF-Bilder sind ein wenig anders als die meisten anderen Bilddateien. Anstatt eine einfache „Dieser Pixel hat jene Farbe“-Information zu enthalten, können WMF-Bilder auf externe Prozesse zurückgreifen. Einer dieser Prozessaufrufe kann zum Ausführen von Schadcode verwendet werden.

- **Sollte ich so etwas wie „DropMyRights“ verwenden um den Schaden gering zu halten?**

Auf jeden Fall ja. Ferner sollten Sie für die tägliche Arbeit nicht als Benutzer mit Administratoren-Rechten angemeldet sein. Allerdings wird dies die Schadenswirkungen nur begrenzen, aber nicht verhindern können. Weiter: Websurfen ist nur eine Möglichkeit, den Schadcode einzufangen. Wenn das Bild auf Ihrem System verbleibt und später von einem Benutzer mit Administrator-Rechten angeschaut wird, wären Sie „befallen“.

- **Sind meine Server verwundbar?**

Möglicherweise... Erlauben Sie das Hochladen von Bildern? E-Mail? Werden diese Bilder indiziert? Verwenden Sie gelegentlich einen Browser auf dem Server? Kurz gesagt: Wenn jemand ein Bild auf Ihren Server bringen kann, und wenn die verwundbare DLL zum Zugriff auf dieses Bild verwendet wird, ist Ihr Server sehr wohl verwundbar.

- **Was kann ich in meinem Sicherheitsbereich tun, um mein Netzwerk zu schützen?**

Nicht viel. Ein Proxy-Server, der alle Bilder von Web-Seiten entfernt? Ihre User werden es Ihnen vermutlich nicht danken. Blockieren Sie zumindest .WMF-Bilder (siehe oben zu Dateiendungen...). Wenn Ihr Proxy einen Virenschanner enthält, könnte der den Schadcode abfangen. Das Selbe gilt für Mailserver. Je weniger ausgehende Verbindungen Sie Ihren Usern erlauben, umso besser. Genaues Überwachen der Workstations könnte zu Hinweisen führen, falls eine Workstation infiziert wurde.

- **Kann ich ein Intrusion Detection System (IDS) verwenden, um den Schadcode zu entdecken?**

Die meisten IDS-Hersteller arbeiten an aktualisierten Signaturen. Kontaktieren Sie Ihren Hersteller/Verkäufer für Details. Bleedsnorting.org bietet einige, sich kontinuierlich verbessernde Signaturen für Snort-Anwender.

- **Wenn ich mir den Schadcode eingefangen habe, was kann ich tun?**

Nicht viel :-). Es hängt sehr davon ab, welchen genauen Schadcode Sie sich eingefangen haben. Die meisten laden zusätzliche Komponenten nach. Es kann sehr hart sein oder sogar unmöglich, alle Teile zu finden. Microsoft bietet kostenfreien Support für Probleme wie diese unter 866-737-2389 (866 PC SAFETY).

[Für Deutschland, Österreich und die Schweiz, verweist Microsoft auf die allgemeine Sicherheitshotline: <http://support.microsoft.com/securityhome?LN=de>]

- **Stellt Microsoft Informationen bereit?**

<http://www.microsoft.com/technet/security/advisory/912840.msp>

Microsoft kündigt darin an, den eigenen, offiziellen Patch am Dienstag, 10. Januar 2006, also dem nächsten regulären „Patch-Day“ zu veröffentlichen.

- **Was sagt das CERT?**

<http://www.kb.cert.org/vuls/id/181038>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>

[Ein weiterer, deutschsprachiger Übersetzungsversuch der WMF-FAQ findet sich unter <http://www.rokop-security.de/index.php?showtopic=10306>]