

# Threat Update: MS Word 0-day Exploit

Lukas Feiler, Achim Brock

25. Mai 2006

Veröffentlichungsdatum d. Sicherheitslücke: 19. Mai 2006  
Betroffene Software: Microsoft Word 2002 und Word 2003  
MITRE CVE-Nummer: CVE-2006-2492  
Bugtraq ID: 18037  
US-CERT Vulnerability Note: VU#446012  
US-CERT Technical Cyber Security Alert: TA06-139A  
Microsoft Security Advisory: 919637  
FrSIRT Advisory: FrSIRT/ADV-2006-1872

## *Inhalt*

1. Einleitung
2. Beschaffenheit der Sicherheitslücke
3. Auswirkungen der Sicherheitslücke
4. Strafrechtliche Beurteilung
5. Technische Gegenmaßnahmen
6. Quellen

## **1. Einleitung**

Microsoft Word ist das am meisten verbreitet Textverarbeitungsprogramm. Die vorliegende Sicherheitslücke betrifft Word 2002 und Word 2003<sup>1</sup> und ist insofern von besonderem Interesse, als dass sie erst durch einen sog „0-day Exploit“ entdeckt wurde. Als Exploit wird ein Werkzeug zur automatisierten Ausbeutung einer Sicherheitslücke bezeichnet. Ein 0-day Exploit, weist die Besonderheit auf, dass er bereits vor dem öffentlichen Bekanntwerden der Sicherheitslücke entwickelt wurde. Dies stellt eine besonders risikoträchtige Situation dar, da zum Zeitpunkt des Auftretens des Exploits noch keine bzw. nur sehr geringe technische Gegenmaßnahmen möglich sind. Es ist jedoch anzumerken, dass bisher offenbar nur eine Organisation angegriffen wurde.<sup>2</sup>

## **2. Beschaffenheit der Sicherheitslücke**

Die vorliegende Sicherheitslücke kann nur dadurch ausgebeutet werden, dass der Angreifer sein Opfer dazu bringt, ein entsprechend präpariertes Word-Dokument zu öffnen. Derzeit verwenden der oder die Angreifer E-Mails mit Word-Dokumenten als Attachment. Folgt der Benutzer der im E-Mail enthaltenen Aufforderung das Attachment zu öffnen, so kommt es in Folge der Öffnung des Dokuments zur Ausnutzung der Sicherheitslücke, wodurch eine Backdoor installiert wird.<sup>3</sup>

Derzeit ist noch äußerst wenig über die Beschaffenheit der Sicherheitslücke bekannt. Die in der National Vulnerability Database<sup>4</sup> enthaltene Beschreibung der Sicherheitslücke lässt jedoch auf einen Buffer Overflow schließen.<sup>5</sup>

---

<sup>1</sup> Nicht hingegen Word 2000; vgl. <http://isc.sans.org/diary.php?storyid=1351>.

<sup>2</sup> vgl <http://isc.sans.org/diary.php?storyid=1345>

<sup>3</sup> Eine Analyse der Backdoor ist unter <http://isc.sans.org/diary.php?storyid=1345> zu finden.

<sup>4</sup> Die National Vulnerability Database wird vom National Institute of Standards and Technology in Zusammenarbeit mit der Cyber Security Division des Department of Homeland Security betrieben.

<sup>5</sup> <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-2492>

### 3. Auswirkungen der Sicherheitslücke

Gelingt es einem Angreifer die Sicherheitslücke auszubeten, so kann er mit den Privilegien des Benutzers beliebige Befehle zur Ausführung bringen. Ist der Benutzer mit administrativen Rechten am System angemeldet, so erlangt der Angreifer uneingeschränkten Systemzugriff.

### 4. Strafrechtliche Beurteilung

Durch die Ausnutzung der Sicherheitslücke erfolgt eine Zugangsverschaffung iSd § 118a StGB. Da ein Buffer Overflow eine Verletzung einer Sicherheitsvorkehrung im Computersystem darstellt, ist der objektive Tatbestand erfüllt, sofern der Angreifer über das System nicht oder nicht allein verfügen darf. Handelt der Angreifer jedoch nicht kumulativ mit Spionage-, Verwendungs- und Gewinn- bzw. Schädigungsabsicht, besteht mangels Erfüllung des subjektiven Tatbestandes keine Strafbarkeit nach § 118a StGB. Beabsichtigt der Angreifer beispielsweise lediglich das System einem Botnet (einem Netzwerk tausender anderer gehackter Systeme) hinzuzufügen und dieses zum Versand von Spam zu verwenden, so tritt keine Strafbarkeit ein. Zur Problematik von Botnet vgl ausführlich *Threat Update: Botnets*.

### 5. Technische Gegenmaßnahmen

Ein Sicherheitsupdate zur Schließung der Sicherheitslücke wird am nächsten Patch-Day<sup>6</sup> von Microsoft bereitgestellt. Bis dahin sollte sichergestellt werden, dass die verwendete Anti-Viren-Software auf dem neuesten Stand ist. Weiters enthält das Microsoft Security Advisory 919637 Anleitungen zur Deaktivierung von MS Word als Mail-Editor und zum Starten von Word im „Safe Mode“.

Für fortgeschrittene Benutzer, die über administrative Rechte verfügen, empfiehlt sich darüber hinaus die Verwendung von DropMyRights<sup>7</sup>.

### 6. Quellen

*Carboni*, Targeted attack: Word exploit – Update, SANS Internet Storm Center, 19. Mai 2006, <http://isc.sans.org/diary.php?storyid=1346>

eEye Security Bulletin, Exploits Circulating for Zero Day Flaw in Microsoft Word, <http://www.eeye.com/html/resources/newsletters/alert/pub/AL20060523.html?sb=kwkmbvmvunbmvambckmn>

*Frantzen*, Targeted attack: experience from the trenches, SANS Internet Storm Center, 18. Mai 2006, <http://isc.sans.org/diary.php?storyid=1345>

*FrSIRT*, FrSIRT/ADV-2006-1872 - Microsoft Word Malformed Object Handling Memory Corruption Vulnerability, <http://www.frstirt.com/english/advisories/2006/1872>

*Goldsmith*, Update on Word 0-Day Issue, SANS Internet Storm Center, 23. Mai 2006, <http://isc.sans.org/diary.php?storyid=1351>

*Internet Security Systems X-Force Database*, Microsoft Word document handling buffer overflow, <http://xforce.iss.net/xforce/xfdb/26556>

Microsoft Security Advisory (919637) - Vulnerability in Word Could Allow Remote Code Execution, 22. Mai 2006, <http://www.microsoft.com/technet/security/advisory/919637.mspx>

---

<sup>6</sup> Patch-Day ist bei Microsoft der zweite Dienstag jedes Monats. Der nächste Patch-Day ist daher am 13. Juni.

<sup>7</sup> <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp>

*Tan*, Microsoft Word Vulnerability, SANS Internet Storm Center, 20. Mai 2006,  
<http://isc.sans.org/diary.php?storyid=1348>

*Toulouse*, Reports of a new vulnerability in Microsoft Word, Microsoft Security Response Center Blog, 19. Mai 2006, <http://blogs.technet.com/msrc/archive/2006/05/19/429353.aspx>

*Toulouse*, A quick check-in on the Word vulnerability, Microsoft Security Response Center Blog, 20. Mai 2006, <http://blogs.technet.com/msrc/archive/2006/05/19/429353.aspx>

*Ullrich*, Word 0-day, recommended defenses, SANS Internet Storm Center, 19. Mai 2006,  
<http://isc.sans.org/diary.php?storyid=1347>