

Threat Update: MS Internet Explorer createTextRange() Vulnerability

SANS Internet Storm Center setzt INFOCon-Level auf “Yellow”

Lukas Feiler, Achim Brock

23. März 2006

Letzte Änderung: 2. April 2006

Veröffentlichungsdatum d. Sicherheitslücke: 22. März 2006

Betroffene Software: Microsoft Internet Explorer 6

MITRE CVE-Nummer: CVE-2006-1359

Bugtraq ID: 17196

US-CERT Vulnerability Note: VU#876678

Secunia Advisory: SA18680

Inhalt

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

1. Einleitung

Microsoft Internet Explorer ist der derzeit, am häufigsten eingesetzte Web-Browser. Den Internet Explorer betreffende Sicherheitslücken sind daher besonders sicherheitskritisch. Zu beachten ist jedoch, dass Sicherheitslücken eines Browsers nur dadurch ausgebeutet werden können, dass der Benutzer dazu gebracht wird, eine vom Angreifer speziell präparierte Website zu besuchen. Weiters ist anzumerken, dass Sicherheitslücken in einem Browser dem Angreifer grundsätzlich nur jene Berechtigungen verschaffen können, über die der Benutzer verfügt. Da in einem betrieblichen Umfeld reguläre Benutzer idR nicht mit administrativen Rechten ausgestattet sind, kann durch die Ausbeutung einer Browser-Sicherheitslücke jedenfalls noch nicht das gesamte Computersystem „übernommen werden“.

Die hier beschriebene Sicherheitslücke stellt eine besondere Gefahr dar, da

- a) sie die Ausführung beliebiger Befehle (mit den Rechten des angemeldeten Benutzers) auf einem verwundbaren System ermöglicht
- b) ein Exploit¹ in den einschlägigen Kreisen bereits veröffentlicht wurde
- c) bislang kein Patch² zur Schließung der Sicherheitslücke zur Verfügung steht.³

Das SANS Internet Storm Center⁴ hat sich daher entschieden den INFOCon-Level⁵ erstmals seit 22. November 2005 auf „yellow“ zu setzen. Dies bringt die, durch diese Sicherheitslücke entstandene erhöhte Gefahrenlage zum Ausdruck.

Secunia⁶, das Unternehmen, das die Sicherheitslücke veröffentlichte, stuft sie ebenso als „Extremely critical“⁷ ein.

¹ Ein Werkzeug zur automatisierten Ausbeutung der Sicherheitslücke.

² Ein Update, das eine Sicherheitslücke schließt.

³ Microsoft arbeitet vorbildlich unter höchstem Zeitdruck an der Herstellung des Patches mit dessen Veröffentlichung uU sogar bereits Dienstag, nächster Woche (4. April 2006) zu rechnen ist.

⁴ <http://isc.sans.org>

⁵ <http://isc.sans.org/infocon.php>

2. Technische Beschaffenheit der Sicherheitslücke

Für ein besseres Verständnis dieser Sicherheitslücke sind einige Kenntnisse der Organisation und das Layouts des Arbeitsspeichers erforderlich. Diesbezüglich sei auf *Feiler*, 26 und *McNab*, 289 ff verwiesen. Die hier zu behandelnde Sicherheitslücke besteht darin, dass ein Instruction Pointer, der auf den nachfolgend auszuführenden Maschinencode (idR im Text-Segment) verweisen müsste in bestimmten Fällen auf (grundsätzlich) nicht existente Bereiche im Heap verweist.⁸ Eine solche Situation kann leicht durch einen zweizeiligen JavaScript-Code herbeigeführt werden.

Der Angriff selbst erfolgt dadurch, dass vor Herbeiführung dieser Situation in jenem Speicherbereich des Heaps auf den dann der Instruction Pointer verweisen wird, der auszuführende Code (sog. „Shell-Code“) platziert wird.

3. Gegenmaßnahmen

Zunächst sollte darauf geachtet werden, dass reguläre Benutzer tatsächlich nicht unnötiger Weise über administrativen Rechte verfügen. Weiters sollte die automatische Update-Funktion von Windows XP aktiviert sein, um den in Kürze von Microsoft zur Verfügung gestellten Patch ohne Verzögerung installieren zu können. Darüber hinaus besteht die Möglichkeit bereits einen Umstieg auf Internet Explorer 7 (derzeit Betaversion) zu tätigen. Internet Explorer 7 ist ebenso wie Internet Explorer 6 kostenfrei verfügbar.⁹

4. Strafrechtliche Beurteilung

Hier soll ausschließlich die Strafbarkeit wegen der Zugangsverschaffung zu einem Computersystem unter Ausnützung dieser Sicherheitslücke erörtert werden. Hierfür kommt grundsätzlich nur § 118a StGB in Betracht. Der objektive Tatbestand erfordert die Zugangsverschaffung zu einem Computersystem durch Verletzung einer Sicherheitsvorkehrung.

Zunächst ist das Vorliegen einer Sicherheitsvorkehrung zu prüfen. Im gegenständlichen Fall implementiert das Programm Internet Explorer die Sicherheitsvorkehrung Least Privilege¹⁰, da es dem Betreiber einer Website grundsätzlich eben nicht möglich ist beliebige Befehle auf dem Computersystem des Clients auszuführen.

Nun bleibt zu prüfen ob es durch die Ausnützung der Sicherheitslücke zu einer Verletzung dieser Sicherheitsvorkehrung kommt. Da das gesamte Programm Internet Explorer dem Prinzip Least Privilege folgend, in seiner Funktionalität beschränkt ist, ist es in seiner Gänze als Sicherheitsvorkehrung zu klassifizieren. Eine Verletzung der Sicherheitsvorkehrung ist daher gleichbedeutend mit der der Beeinträchtigung der Datensubstanz des Programms Internet Explorer. Es gilt daher festzustellen ob das Programm Internet Explorer durch die Ausnützung der Sicherheitslücke in seiner Substanz verletzt wird. Der erste Schritt des Angriffs besteht darin, den auszuführenden Maschinencode in bislang unbenutzte Speicherbereiche zu laden. Da es hierbei zu keinem Überschreiben von Daten kommt, die als Teil des Internet Explorers zu klassifizieren wären, liegt in diesem Stadium jedenfalls keine Verletzung vor. Im zweiten Schritt des Angriffs wird ein zweizeiliger JavaScript-Code ausgeführt, der einen Programmfehler verursacht, wodurch ein Instruction Pointer auf einen (zuvor vom Angreifer befüllten) Bereich des Heaps zeigt. In diesem zweiten Schritt kommt es auch zu keinem Überschreiben von Daten. Es wird lediglich ein Fehler im Programm ausgenutzt, der dieses in einen, nicht vom Programmierer beabsichtigten Status zurücklässt.

⁶ <http://secunia.com>

⁷ http://secunia.com/about_secunia_advisories/

⁸ so <http://marc.theaimsgroup.com/?l=full-disclosure&m=114310434227531&w=2>

⁹ <http://www.microsoft.com/windows/IE/ie7/default.aspx>

¹⁰ *Garfinkel/Spafford/Schwartz*, Practical Unix & Internet Security³, 235, O'Reilly, Sebastopol 2003; *Feiler*, 14 f

Da es weder im ersten, noch im zweiten Schritt des Angriffs zum Überschreiben von Programmdateien kommt, ist die Verletzung einer Sicherheitsvorkehrung iSd § 118a StGB zu verneinen. Die **Zugangsverschaffung zu einem Computersystem unter Ausnützung dieser Sicherheitslücke** ist daher – ungeachtet des (erweiterten) Vorsatzes – **nicht nach § 118a StGB strafbar**.

Der Vollständigkeit halber sollen nun folgend auch die Voraussetzungen für eine Strafbarkeit nach dem Zugangskontrollgesetz (ZuKG) erörtert werden. Dieses schützt im Bereich der Informationstechnologie gem § 2 Z 2 ZuKG jedoch nur Dienste der Informationsgesellschaft, die gegen Entgelt und unter einer Zugangskontrolle erbracht werden. Kostenfrei angebotene Dienste oder gar für private Zwecke eingesetzte Computersysteme fallen daher jedenfalls nicht in den Anwendungsbereich des ZuKG. Zweck der Strafbestimmungen des ZuKG ist es den Handel mit Umgehungsvorrichtungen iSd § 2 Z 8 ZuKG zu unterbinden. Es handelt sich hierbei um Geräte bzw. Computerprogramme, die den Zugang zu einem geschützten Dienst ohne Erlaubnis des Anbieters ermöglichen. Gem § 10 Abs 1 ZuKG wird nur strafbar, wer Umgehungsvorrichtungen gewerbsmäßig (iSd § 70 StGB) vertreibt, verkauft, vermietet oder verpachtet. Gem § 10 Abs 2 ZuKG wird ebenso strafbar wer gewerbsmäßig Umgehungsvorrichtungen herstellt, einführt oder mit dem Vorsatz erwirbt oder innehat, dass diese auf die im Abs. 1 beschriebene Art und Weise in Verkehr gebracht werden oder dass mit ihrer Hilfe anderen der Zugang zu einem geschützten Dienst ermöglicht wird.

Der sich ausschließlich selbst Zugang verschaffende Täter wird daher nur dann strafbar, wenn er gewerbsmäßig handelt und die Umgehungsvorrichtung selbst hergestellt oder eingeführt hat.

Da die Ausnützung der hier beschriebenen Sicherheitslücke des Internet Explorers nur in den ausgefallensten Fallkonstellationen den Zugang zu einem gegen Entgelt erbrachten Dienst der Informationsgesellschaft ermöglicht, bleibt es grundsätzlich bezüglich der Zugangsverschaffung durch Ausnützung der beschriebenen Sicherheitslücke bei einer Strafflosigkeit.

5. Rechtspolitische Anmerkungen

Die Unfähigkeit des österreichischen Strafrechts hinreichenden Schutz vor dieser äußerst erheblichen Bedrohung für die IT-Sicherheit zu gewähren, sollte zum Anlass genommen werden die Sinnhaftigkeit des Tatbestandsmerkmals der Verletzung einer Sicherheitsvorkehrung zu überdenken.

6. Quellen

CVE-2006-1359

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-1359>

US-CERT Vulnerability Note VU#876678,

<http://www.kb.cert.org/vuls/id/876678>

SecurityFocus Bugtraq ID 17196,

<http://www.securityfocus.com/bid/17196>

Secunia Advisory SA18680,

<http://secunia.com/advisories/18680/>

Computer Terrorism (UK) Security Advisory CT22-03-2006,

<http://www.computerterrorism.com/research/ct22-03-2006>

Microsoft Security Advisory (917077)
<http://www.microsoft.com/technet/security/advisory/917077.msp>

Microsoft Security Response Center Blog,
<http://blogs.technet.com/msrc/archive/2006/03/22/422849.aspx>
<http://blogs.technet.com/msrc/archive/2006/03/25/423116.aspx>

Clausing, IE exploit on the loose, going to yellow, SANS Internet Storm Center,
<http://isc.sans.org/diary.php?storyid=1212>

Bueno, Updates on IE vulnerability, SANS Internet Storm Center,
<http://isc.sans.org/diary.php?storyid=1223&rss>

Nolan, Email attachment vector for IE createTextRange() Remote Command Execution, SANS Internet Storm Center,
<http://isc.sans.org/diary.php?storyid=1222&rss>

Hutcheson, Modified Malware for the IE Exploit, SANS Internet Storm Center,
<http://isc.sans.org/diary.php?storyid=1221&rss>

Dokumentation der Methode createTextRange(),
<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/createtextrange.asp>

McNab, Network Security Assessment, O'Reilly, Sebastopol 2004

Feiler, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 2006

Garfinkel/Spafford/Schwartz, Practical Unix & Internet Security³, 235, O'Reilly, Sebastopol 2003

Mediale Berichterstattung

Neue "extrem kritische" und "offene" Sicherheitslücke im Internet Explorer, derStandard.at, 27. März 2006,
<http://derstandard.at/?url=/?id=2389144>

Gefährdung durch Internet Explorer-Lücke wird äußerst real, derStandard.at, 27. März 2006,
<http://derstandard.at/?url=/?id=2391809>

Brian Krebs, Attacks on Unpatched IE Flaw Escalate, washingtonpost.com, 27. März 2006,
http://blog.washingtonpost.com/securityfix/2006/03/attacks_on_internet_explorer_f_1.html

Farrell, Microsoft plans April 11 for super critical IE bug fix, www.theinquirer.net, 28. März 2006,
<http://www.theinquirer.net/?article=30583>