Pressemitteilung

Millionen Anwender durch schwere, kritische Sicherheitslücke in Microsofts Outlook in Gefahr

Sankt Augustin, 7. Mai 2014

Angriffsrisiko durch XML-Bombe seit 2009 Microsoft-intern bekannt

Microsoft wartet mit einem Patch

Angreifer können PCs, auf denen Outlook 2007–2013 installiert ist, regelrecht zum Einfrieren bringen. Nichts geht dann mehr mit Outlook. Die dafür notwendige XML-Bombe besteht aus nur wenigen Zeilen einer E-Mail (HTML- oder Nur-Text) und nutzt eine Sicherheitslücke im Zusammenhang mit der Seitenbeschreibungssprache XML aus. „Explodiert die XML-Bombe in einem PC, friert Outlook ein. Je nach Konfigurierung ist ein Neustart von Outlook gar nicht möglich", erläutert softScheck-Geschäftsführer Professor Dr. Hartmut Pohl. Selbst Sicherheitseinstellungen schützen nicht gegen das Einfrieren von Outlook.

Der PC-Anwender muss zunächst die betreffende Mail mit der XML-Bombe löschen. Um das tun zu können, muss Outlook im abgesicherten Modus gestartet werden. Viele PC-Anwender sind damit überfordert und der XML-Bombe deshalb mehr oder weniger hilflos ausgeliefert.

Mitarbeiter der IT-Sicherheitsberatung softScheck in Sankt Augustin bei Bonn hatten die kritische Denial of Service Sicherheitslücke in Outlook bei einem Standardtest entdeckt und Microsoft bereits im Februar 2014 darüber informiert. Das Microsoft Security Response Center hat die Sicherheitslücke bestätigt, bis heute allerding nicht geschlossen. „Unsere weiteren Recherchen haben dann ergeben, dass dieses Sicherheitsproblem Microsoft-intern bereits seit dem Jahr 2009 bekannt ist", berichtet softScheck-Chef Pohl.

Um das Problem zu beheben und die Sicherheitslücke zu schließen, muss Microsoft beim sogenannten XML-Parser nachbessern. Das ist ein Computerprogramm, das in der Seitenbeschreibungssprache XML erstellte Dokumente analysiert und für die weitere Bearbeitung aufbereitet.

Als Soforthilfe empfiehlt softScheck Outlook-Anwendern, Mails mit der Dokumententyp-Definition („<!ENTITY") vom Spam-Filter herausfischen zu lassen.

Die Sicherheitslücke ist geeignet für Gegenangriffe. Angegriffene amerikanische Sicherheitsbehörden wie die NSA verteidigen sich bei Angriffen mit Gegenangriffen (Counter Attack by Sabotage).

Über softScheck

Die IT-Sicherheitsberatung softScheck GmbH hat sich in den letzten Jahren mit der Identifizierung von bisher nicht-erkannten Sicherheitslücken in Software (und auch Hardware) neue, attraktive Wachstumsfelder erschlossen.

softScheck führt regelmäßig Sicherheitsprüfungen von Software und Hardware durch. Daneben bietet softScheck selbstverständlich auch die klassische IT-Sicherheitsberatung an vom Grundschutz (ISO 27000-Familie) bis hin zur Hochsicherheit in der Informationsverarbeitung (Redundanz und Diversität) – auch mit Consulting, Coaching und Forensics.

Kontakt

Anja Wallikewitz
Tel.: 02241 – 255 43 – 11
Fax: 02241 – 255 43 – 29
anja.wallikewitz@softScheck.com

softScheck GmbH
Bonner Straße 108
53757 Sankt Augustin
www.softScheck.com

softScheck
we identify vulnerabilities others don't

Sicherheitslücke in Microsofts Outlook: Technischer Hintergrund

Werden die Inhalte von E-Mails mit der XML-Bombe im Lesebereich angezeigt, stürzt Outlook beim Starten ab. Die Sicherheitslücke betrifft den XML-Parser der Microsoft Office Produkte (inklusive Word und generell Office für Mac). Der Parser kann mit einer XML-Bombe zum Bearbeiten einer exponentiell wachsenden Aufgabe gezwungen werden. Damit wird der Arbeitsspeicher zunehmend gefüllt und die Anwendung friert ein.

Das grundsätzliche Problem der Denial of Service Attacks ist seit mindestens 2003 bekannt und wurde von Microsoft seit 2009 in mehreren Artikeln[1] thematisiert.

Die Sicherheitslücke betrifft den XML-Parser von Microsoft Office und damit auch andere Microsoft Office Produkte. Seit Microsoft Office 2007 verwenden alle Office-Produkte (also auch Word) auf XML basierende Dateiformate und sind damit in allen Versionen und Patch-Level für diese Lücke anfällig. Der XML-Parser kann mit einer XML-Bombe zum Abarbeiten einer exponentiell wachsenden Aufgabe gezwungen werden, was den Arbeitsspeicher zunehmend füllt und die Anwendung zum Einfrieren bringt.

Das Öffnen einer Text-Email mit folgendem Inhalt bringt Outlook zum Einfrieren:

```
<?xml version="1.0"?>
<!DOCTYPE bomb [
<!ELEMENT bomb (#PCDATA)>
<!ENTITY a "aaaaaaaaaaaaaaaa">
<!ENTITY b "&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;&a;">
<!ENTITY c "&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;&b;">
<!ENTITY d "&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;&c;">
<!ENTITY e "&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;&d;">
<!ENTITY f "&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;&e;">
<!ENTITY g "&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;&f;">
<!ENTITY h "&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;&g;">
<!ENTITY i "&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;&h;">
<!ENTITY j "&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;&i;">
<!ENTITY k "&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;&j;">
<!ENTITY l "&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;&k;">]>
<bomb>&l;</bomb>
```

Darin werden mittels einer XML Dokumenttypdefinition (DTD) mehrere Entitäten definiert, die jeweils rekursiv auf die Vorhergehenden verweisen. Ein XML-Parser ist darauf angewiesen, alle Verweise zu expandieren, was eine exponentiell wachsende Aufgabe ist während der Outlook einfriert. Zwar kehrt nach der Verarbeitung Outlook zu einem lauffähigen Status zurück, doch dies dauert Tage und kann durch Erweitern der XML-Bombe um wenige Zeichen auf Monate hochgeschraubt werden.

[1] Sullivan, B.: XML Denial of Service Attacks and Defenses. MSDN http://msdn.microsoft.com/en-us/magazine/ee335713.aspx