IT-Sicherheit

Kritische Lücke in Microsoft Office ermöglicht Remote Code Execution

12. Oktober 2017

Researcher haben eine schwerwiegende Sicherheitslücke in Microsoft Office entdeckt.

Wenn ein Benutzer eine speziell präparierte Datei im Microsoft Excel-Format oder Microsoft Word-Format öffnet, kann in Folge ein Angreifer beliebigen Code, mit den Rechten des angemeldeten Benutzers, auf dem System ausführen.

Die Schwachstelle basiert auf der Verwendung von Dynamic Data Exchange (DDE), einem Protokoll zum Austausch von Daten zwischen Applikationen, welches von Excel verwendet wird, um externe Informationen einzubinden. Das Filtern von Makros oder der Einsatz von restriktiven Policies bezüglich der Verwendung von VBA bieten dementsprechend keine Abhilfe.

Gezielte Angriffe scheinen aktuell bereits durchgeführt zu werden. Da die Methode nun öffentlich bekannt ist, ist anzunehmen, dass entsprechende Dateien bald massenhaft per zB Spam-Mail verteilt werden.

Auswirkungen

Über diesen Fehler kann potentiell beliebiger Code auf den betroffenen Systemen ausgeführt werden. Es sind alle Daten auf diesen Systemen, sowie potentiell alle durch diese erreichbaren (etwa durch Login, VPN etc.) Daten und anderen Systeme gefährdet.

Betroffene Systeme

Die Researcher geben an, dass alle Versionen von Microsoft Office, inkl. Office 2016 auf Windows 10, für diese Lücke anfällig sind.

Abhilfe

Es stehen noch keine Updates zur Verfügung.

Da das Öffnen von Dokumenten mit eingebundenen DDE-Elementen dem Benutzer im Normalfall zwei Sicherheitswarnungen präsentiert macht es Sinn, gesondert darauf hinzuweisen, Informationsfenster aktuell besonders kritisch zu betrachten, und sich bei etwaigen Unsicherheiten und Verdachtsfällen an die IT-Kontaktperson des Instituts zu wenden.

In diesem Zusammenhang weisen wir auch wieder darauf hin, dass durch das Entfernen von Administratorrechten, die für die tägliche Benutzung nicht notwendig sind, viele Angriffe vermieden werden könnten!

Computersicherheit ist ein wichtiges Thema, nicht nur für Server sondern auch für Arbeitsplätze.

Unsere Aufgabe sehen wir darin, Angriffen gegen die Sicherheit (Hackerattacken, Virenverseuchung etc.) entgegenzuwirken. Ebenso bieten wir Hilfe nach einem Hackerangriff oder einem Virenbefall an.

Weiters möchten wir unsere Erfahrungen und den Gebrauch von geeigneten Gegenmaßnahmen hier publizieren. Der

ZID bietet auch umfangreiche Hilfe in Form von Plattform Unterstützung für Server und Arbeitsplätze an.

Durch das immer schnellere Bekanntwerden von Sicherheitslücken, welche die Hacker ausnutzen, ist ein möglichst schnelles Installieren von Patches notwendig. Daher sollten die bei allen gängigen Plattformen vorhandenen Update-Dienste regelmäßig benutzt werden.

Der beste Beitrag zur Sicherheit ist sicherlich die Prävention - wenn ein Rechner einmal gehackt ist, bedeutet dies meistens eine Neuinstallation. Um das zu vermeiden, hier ein paar Tipps:

- Keine offenen Dienste ohne Passwörter oder default Passwörter, nur die Dienste auf dem Rechner installieren, die wirklich benötigt werden.
- Keine unsicheren Logins per Telnet, sondern SSH verwenden. Wir empfehlen frei erhältliche Software (SSH-Clients wie puTTY, WinSCP oder Virenscanner wie Avira und Avast in der jeweiligen Free-Variante, etc.), vgl. z. B. Campus-Software-Angebot.
- Diese Dienste immer auf dem neuesten Versionsstand halten, bei Windows Clients: immer Virenscanner und auch Trojanerscannner installieren (am besten mit Internetupdatefunktion).
- Bei Neuinstallation Checksummen aller Programme auf ein externes Medium speichern (bei Änderungen diese Daten auf dem externen Medium aktualisieren).
- Logfiles auch auf einen externen Rechner speichern, da Hacker auf dem angegriffenen Rechner ihre Spuren verwischen.
