Pressemitteilung

Sankt Augustin, 14. Okt. 2014

SQL-Injection in Open-Xchange Server / OX AppSuite

softScheck hat in der Open-Source E-Mail und Groupware-Lösung Open-Xchange der Open-Xchange AG eine schwerwiegende Sicherheitslücke des Typs SQL-Injection identifiziert. Ein Angreifer mit einem regulären Benutzer Account kann beliebige Daten aus der Datenbank auslesen und je nach Konfiguration Kontrolle über den Server erlangen.

CVE-ID: CVE-2014-7871

CVSS-Bewertung: 7.6

Details

Die Sicherheitslücke betrifft:

- Open-Xchange App Suite / OX 6 backend 7.6.0-rev22 oder älter
- Open-Xchange App Suite / OX 6 backend 7.4.2-rev35 oder älter

Eine API des Open-Xchange Backends ist für SQL-Injections in jedem der übergebenen JSON-Werte anfällig. Ein XMLHttpRequest mittels PUT mit modifiziertem JSON-Parameter resultiert in Ausführung des injizierten SQL-Befehls. Auch ein unregelmäßiger GET-Request mit angehängten Daten kann für die SQL-Injection verwendet werden. Da die API bei einer gültigen Anfrage keine Ausgabe liefert, muss die SQL-Injection so formuliert werden, dass die gewünschte Abfrage in einer Fehlermeldung wiedergegeben wird.

Auswirkungen

Jeder Benutzer des Systems kann über die Lücke beliebige Daten aus der Datenbank wie z.B Inhalte von E-Mails, Passworte oder Passworthashes auslesen und schreiben. Ebenfalls können Daten aus dem Dateisystem des Servers gelesen werden. Abhängig von der Konfiguration kann die Lücke in eine Übernahme des Servers resultieren.

Schutzmaßnahmen

Die Sicherheitslücke wurde zeitnah mit Patch Release #2213 behoben. softScheck GmbH empfiehlt dringend den Patch aufzuspielen.

Timeline

07.10.2014 Meldung der Lücke

08.10.2014 Patch Release #2213

Über softScheck

Die IT-Sicherheitsberatung softScheck GmbH hat sich in den letzten Jahren mit der Identifizierung von bisher nicht-erkannten Sicherheitslücken (Zero-Day-Vulnerabilities) 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

Mahtab Delschad
Tel.: 02241 – 255 43 – 0
Fax: 02241 – 255 43 – 29
mahtab.delschad@softScheck.com

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