REPORT: CYBERKRIMINELLE LIEBEN ÄLTERE SICHERHEITSLÜCKEN

Posted on 10.08.2023 by UKramer40878

Category: Cyber

(Bild: Dmitry Demidovich/Shutterstock.com) Unter anderem die US-Institutionen Cybersecurity and Infrastructure Security Agency (CISA) und FBI zeigen mit weltweiten Partnern wie dem Cyber Security Centre (NCSC-UK) in einem Report auf, dass Online-Gangster überwiegend schon länger bekannte Sicherheitslücken ausnutzen, um Unternehmen zu attackieren. Alt, aber nicht minder gefährlich

Wie aus dem Report über die im Jahr 2022 am häufigsten ausgenutzten Schwachstellen hervorgeht , läuft das Patch-Management in vielen Firmen offensichtlich nicht optimal: Viele der ausgenutzten Lücken stammen aus den Vorjahren. Den Großteil bilden Sicherheitslücken aus dem Jahr 2021. Einige gehen sogar bis ins Jahr 2017 zurück.

Im Jahr 2022 wurden im Zuge des Common-Vulnerabilities-and-Exposures-Programm (CVE) über 25.000 neue Sicherheitslücken gemeldet. Davon tauchen in der Top zwölf der 2022 am häufigsten ausgenutzten Lücken nur fünf Stück in der Liste auf.

Dem technischen Direktor der NSA Neal Ziring zufolge bieten ältere Schwachstellen Angreifern einen kostengünstigen und wirkungsvollen Ansatzpunkt, um auf sensible Daten zuzugreifen. Da die Lücken schon länger bekannt sind, sind sie gut dokumentiert und Exploitcode ist bereits über einen längeren Zeitraum in Umlauf. So fallen Attacken leichter und Angreifer scannen das Internet kontinuierlich nach verwundbaren Systemen – und landen, wie der Report zeigt, auch Jahre später noch Treffer. Jetzt patchen!

Besonders beliebt bei Angreifern ist nach wie vor eine fünf Jahre alte Lücke (CVE-2018-13379) in FortiOS und FortiProxy. Darüber können Angreifer VPN-Zugangsdaten abgreifen. Auch die Proxy-Shell-Schwachstellen in Microsoft Exchange (CVE-2021-34473, CVE-2021-31207, CVE-2021-34523) sind nach wie vor gefragt. In diesen Fällen können Angreifer unter anderem Schadcode ausführen. Eine Exchange-Lücke (CVE-2017-11882) geht sogar bis ins Jahr 2017 zurück.

Viele der genannten Schwachstellen dominierten die Liste auch bereits im Jahr 2022 für die im Jahr 2021 am häufigsten ausgenutzten Lücken . Auch wenn es für viele Admins wie eine Selbstverständlichkeit klingt, sollten Sicherheitspatches stets zeitnah installiert werden.

Darüber hinaus sollten sie ihre Systeme gezielt auf ältere Schwachstellen analysieren und umgehend handeln. In einem Beitrag geben die Autoren des Reports noch weitere Sicherheitstipps, wie Admins sich der gefährlichen Altlasten entledigen können .