

Telefonanbieter konnte Schwachstelle in seinen Systemen mit Hilfe des ICT-Sicherheitsspezialisten beseitigen

Compass hat Sicherheitslücke in VoIP-Telefonen von Snom entdeckt

Rapperswil, 13. August 2009 – Bereits im vergangenen Jahr kursierten Meldungen über eine Schwachstelle in den VoIP-Telefonen des Herstellers Snom. Hierbei handelte es sich um Cross-Site Request Forgery, die es Angreifern erlaubt, Adressbucheinträge und Anrufprotokolle zu ändern sowie Gespräche abzuhören. Snom reagierte mit Maßnahmen, um den Schutz der Produkte zu optimieren. Die Compass Security AG, ICT-Sicherheitsspezialist, hat daraufhin eine weitere Lücke im System ausgemacht und gemeldet, so dass diese behoben werden konnte.

Cross-Site Request Forgery ermöglicht es dem Angreifer, unberechtigt Daten in einer Webanwendung zu verändern und Vollzugriff auf das Endgerät zu erhalten. Somit wird unter anderem das Abhören der Gespräche ermöglicht. Snom hatte zur Verhinderung der Attacke empfohlen, einen Benutzernamen und Passwort für das Webinterface zu definieren. Compass hat jedoch herausgefunden, dass die Authentisierung nicht korrekt implementiert war. Durch einfache Manipulation des http-Requests wird sie vollständig ausgehebelt. Der Angreifer kann somit ohne Kenntnisse bezüglich des Passwortes auf das Webinterface des Telefons zugreifen und dieses vollständig kontrollieren.

Walter Sprenger, Geschäftsführer der Compass Security AG in der Schweiz, hat die Schwachstelle entdeckt und erklärt: „Durch die Verwundbarkeit dieses Voice over IP-Telefons ist eine Lawful Interception für Dummies möglich.“ Das bedeutet, dass der gesamte Netzwerk-Verkehr erfasst und Gespräche abgehört werden können. Der Zugriff auf sensible Adressbuchdaten wird ebenso ermöglicht wie das Anrufen kostenpflichtiger Dienste. Darüber hinaus können der SIP-Benutzername und das Passwort sowie alle Konfigurationen des Telefons eingesehen und verändert werden. Angreifer erhalten außerdem die Möglichkeit, Gespräche zu einem anderen VoIP-Server umzuleiten und eine stille Raumüberwachung durch Aktivieren des Mikrofons durchzuführen.

Sicherheitsproblem erkannt und gebannt

Compass hat alle Erkenntnisse umgehend an den Hersteller weitergeleitet, dem die Sicherheitslücke bereits bekannt war. Sie war jedoch noch nicht in allen Firmware-Main-Versionen behoben und den Kunden nicht gemeldet. Snom konnte die Schwachstelle im letzten Update fixen und somit das Problem beheben. Es wird empfohlen, mindestens die Firmware-Versionen 6.5.20, 7.1.39, 7.3.14 oder höher zu installieren.

Weitere Informationen zur Security Advisory unter:

<http://www.csnc.ch/en/downloads/advisories.html>

Kurzporträt Compass Security AG:

Die 1999 gegründete Compass Security AG mit Sitz in Rapperswil (CH) hat sich als europäisches Dienstleistungsunternehmen auf Security-Assessments zur Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmensdaten spezialisiert. Mittels Penetrationstests, Ethical Hackings und Reviews beurteilt Compass ICT-Lösungen hinsichtlich Sicherheitsrisiken präventiv, spürt vorhandene Schwachstellen auf und unterstützt bei deren Beseitigung. IT-forensische Experten ermöglichen durch Erfassung, Prüfung und Auswertung digitaler Spuren die Rekonstruktion und beweisdienliche Dokumentation von Missbrauchsfällen im Zusammenhang mit digitalen Systemen. Praxisnahe Workshops und Schulungen zum Thema IT-Security sowie Live-Hacking-Vorträge zur Usersensibilisierung runden das Portfolio ab. Neutralität und Produktunabhängigkeit sind dabei wesentliche Bestandteile der Unternehmensphilosophie. Der Kundenstamm setzt sich aus nationalen und internationalen Kunden jeglicher Größenordnung und unterschiedlicher Branchen zusammen. Weitere Informationen unter: www.csnc.ch

Weitere Informationen:

Compass Security AG
Postfach 1628
Glärnischstrasse 7
CH-8640 Rapperswil

Tel.: +41 55 214 41 60

Fax: +41 55 214 41 61

www.csnc.ch

PR-Agentur:

Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau

Ansprechpartner:

Ulrike Peter
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: up@sprengel-pr.com
www.sprengel-pr.com