Falla nella piattaforma Cisco UCCE mette a rischio la privacy degli utenti

Gen 17, 2022 Marco Schiaffino In evidenza, News, Vulnerabilità 0

Il sistema di assistenza clienti è affetto da una vulnerabilità che consentirebbe la compromissione della piattaforma. Ecco come funziona.

La gravità della falla è testimoniata da un indice di rischio di 9.6 su 10 e permetterebbe a un pirata informatico di prendere il controllo del sistema di gestione dell'assistenza clienti di **Cisco UCCE**.

L'allarme è stato lanciato direttamente dall'azienda produttrice, che in un report pubblicato su Internet descrive i dettagli della vulnerabilità (CVE-2022-20658) che interessa il servizio **Unified Contact Center Enterprise**.

Si tratta di un sistema on premise che consente di gestire fino a 24.000 agent dedicati al customer service, con funzionalità IVR (Interactive Voice Response), gestione delle email, chiamate e quanto altro si possa immaginare in ambito assistenza clienti.

Il problema riguarda la possibilità che un utente autenticato possa eseguire un processo di elevazione di privilegi ottenendo il ruolo di amministratore e la possibilità di creare nuovi amministratori nel sistema.

Advisory ID:	cisco-sa-ccmp-priv-esc-JzhTFLm4
First Published:	2022 January 12 16:00 GMT
Version 1.0:	Final
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCvz49473
CVSS Score:	Base 9.6

Download CVRF

Email

Nel dettaglio, il bug riguarda il fatto che sia **Cisco Unified Contact Center Management Portal (Unified CCMP)**, sia **Cisco Unified Contact Center Domain Manager (Unified CCDM)** utilizzano un sistema di autenticazione che viene eseguito lato client, consentendone la violazione.

Una volta ottenuta l'autenticazione, un pirata informatico può gestire con la massima libertà tutte le funzionalità gestite dal CCDM con la conseguente possibilità sia di rubare informazioni relative ai clienti, sia di provocare danni a livello di reputazione all'azienda.

L'unico elemento di conforto è che per portare l'attacco è necessario avere a disposizione l'accesso a un account Cisco UCCE, anche se con privilegi limitati.

L'aggiornamento che corregge la vulnerabilità è disponibile attraverso la piattaforma di Cisco, che (naturalmente) invita "caldamente" tutti gli utenti ad aggiornare il software.

Condividi l'articolo

Microsoft non si muove: patch "ufficiosa" per la falla Remote Potato0

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2022/01/17/falla-nella-piattaforma-cisco-ucce-mette-a-rischio-la-privacy-degli-utenti/?utm_source=rss&utm_medium=rss&utm_campaign=falla-nella-piattaforma-cisco-ucce-mette-a-rischio-la-privacy-degli-utenti