Computer Emergency Response Team

BOLLETTINO IT-CERT.180503.B01

Vulnerabilità critica in Cisco WebEx Network Recording Player (CVE-2018-0264)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

Cisco WebEx è una piattaforma per videoconferenze, riunioni a distanza, condivisione di documenti e applicazioni, chiamate VoIP. I *player* di Cisco WebEx sono applicazioni che consentono di visualizzare registrazioni di riunioni a distanza effettuate da uno dei partecipanti. Questi *player* possono essere installati automaticamente quando un utente accede al file di una registrazione ospitato su un server WebEx.

È stata scoperta una vulnerabilità critica (CVE-2018-0264) in applicazioni **Cisco WebEx Network Recording Player** per file nel formato *Advanced Recording Format* (ARF). Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità facendo in modo che l'utente di un *player* affetto apra un file ARF appositamente predisposto inviato via Email o scaricato da un URL malevolo. Se sfruttata con successo, questa vulnerabilità può consentire all'attaccante di eseguire codice arbitrario sul sistema sottostante.

Al momento non ci sono notizie che questa vulnerabilità sia stata sfruttate in attacchi reali.

Cisco ha rilasciato aggiornamenti software che risolvono le vulnerabilità nei prodotti interessati. Non sono disponibili soluzioni alternative per mitigare queste vulnerabilità (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

La vulnerabilità descritta in questo bollettino è stata risolta nei *client* inclusi nelle seguenti versioni dei prodotti **Cisco WebEx Business Suite**, **Cisco WebEx Meetings** e **Cisco WebEx Meetings Server**:

- Cisco WebEx Business Suite (WBS31) *client build* T31.23.4 e successive
- Cisco WebEx Business Suite (WBS32) *client build* T32.12 e successive
- Cisco WebEx Meetings con *client build* T32.12 e successive
- Cisco WebEx Meeting Server *build* 3.0 *Patch* 1 e successive

I gestori di sistemi Cisco WebEx devono installare gli aggiornamenti relativi alla propria piattaforma, dopo appropriato *testing*.

Per maggiori informazioni sui prodotti vulnerabili e sugli aggiornamenti disponibili, si raccomanda di consultare il relativo bollettino di sicurezza di Cisco (si veda la sezione LINK UTILI).

SISTEMI

Risultano affetti dalla vulnerabilità CVE-2018-0264 i *client* inclusi nelle seguenti versioni dei prodotti **Cisco WebEx Business Suite**, **Cisco WebEx Meetings** e **Cisco WebEx Meetings Server**:

- Cisco WebEx Business Suite (WBS31) *client build* precedenti la T31.23.4
- Cisco WebEx Business Suite (WBS32) *client build* precedenti la T32.12
- Cisco WebEx Meetings con *client build* precedenti la T32.12
- Cisco WebEx Meeting Server *build* precedenti la 3.0 *Patch* 1

LINK UTILI

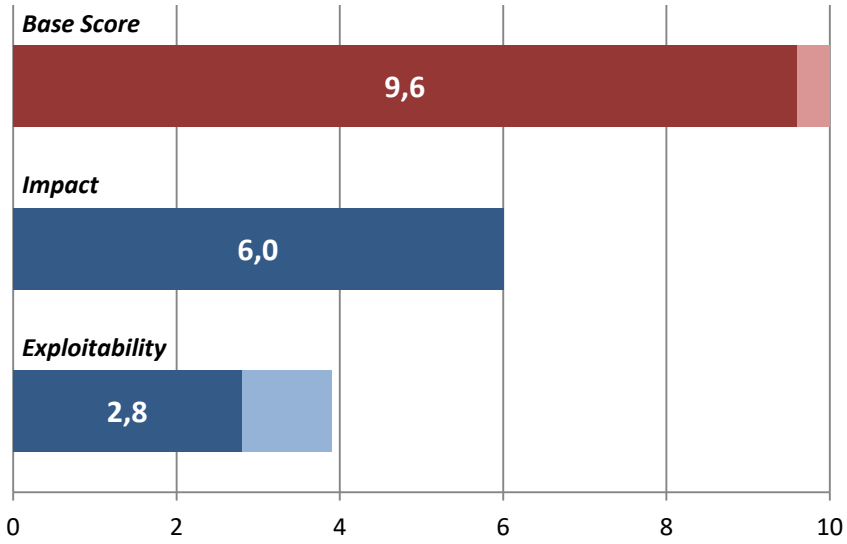
Avviso del produttore

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180502-war

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0264

VALUTAZIONE CVSS



Relativamente alla valutazione della *severity* come metrica di base - da intendersi quale livello di pericolosità della vulnerabilità delle componenti di sistema o delle piattaforme - il CERT Nazionale valuta i parametri che concorrono al calcolo della *Base Score* secondo lo standard CVSS v3 (*Common Vulnerabilities Scoring System*), avvalendosi del *tool* messo a disposizione dal sito del NIST (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).

Nello specifico, per le più gravi delle vulnerabilità oggetto di questo bollettino, sono stati raggiunti i seguenti punteggi:

- *Base Score:* 9,6
- *Impact:* 6,0
- *Exploitability:* 2,8

Vettore CVSS: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

NOTE

Le informazioni contenute nel presente bollettino sono fornite a meri fini informativi.

In nessun caso il CERT Nazionale può essere ritenuto responsabile di qualunque perdita, pregiudizio, responsabilità, costo, onere o spesa, ivi comprese le eventuali spese legali, danno diretto, indiretto, incidentale o consequenziale, derivante da o connesso alle informazioni riportate nel presente bollettino.

La versione PDF del bollettino è statica ed, in quanto tale, contiene le informazioni disponibili al momento della pubblicazione.