Infrastrutture critiche a rischio: il bug è nelle VPN

Lug 29, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Le falle di sicurezza nei sistemi di controllo in remoto mettono a rischio i sistemi industriali. L'allarme lanciato dagli esperti del settore.

Aumentano le preoccupazioni per la possibilità di attacchi informatici ai danni dei sistemi industriali e, in particolare, alle infrastrutture che gestiscono servizi critici come energia, erogazione dell'acqua e trasporti.

Gli allarmi più recenti fanno riferimento alle falle di sicurezza che interessano i sistemi di controllo remoto e, in particolare, le VPN (Virtual Private Network) utilizzate per accedere ai sistemi che gestiscono le infrastrutture.

Secondo quanto riporta il **Claroty Research Team** in un report pubblicato sul blog ufficiale della società di sicurezza specializzata in analisi dei sistemi IT/OT, nelle ultime settimane sono emerse una serie di vulnerabilità che suscitano serie preoccupazioni riguardo alla possibilità di futuri attacchi.

IL primo squillo ha riguardato una vulnerabilità (CVE-2020-14511) relativa ai router **Moxa** della serie **EDR-G902** ed **EDR-G903**. A seguire, sono arrivati indizi sulle falle di sicurezza dei prodotti di **Secomea** e **HMS Networks**.

Insomma: stiamo parlando di dispositivi e sistemi che vengono utilizzati per gestire i collegamenti in remoto di infrastrutture complesse dedicate alla gestione di impianti

industriali.

Le vulnerabilità scoperte da **Sharon Brizinov** e **Tal Keren** consentirebbero, in pratica, di sfruttare una connessione remota per avviare l’esecuzione di codice sui dispositivi.

La collezione di bug individuati dai ricercatori comprende alcune falle di sicurezza che potrebbero essere sfruttate utilizzando come vettore di attacco una semplice mail.

Qualcosa di estremamente preoccupante, come il **Proof of Concept** (PoC) pubblicato in video che dimostra ocme sia possibile sviluppare uno strumento di compromissione che funziona con una semplicità disarmante.
[embedded content]

Claroty Demo Video of Secomea GateManager CVE-2020-14500 Exploit from BleepingComputer.com on Vimeo.

In conclusione, il tema della vulnerabilità delle infrastrutture critiche a eventuali attacchi informatici dimostra di essere più caldo che mai. E il fatto che i punti deboli siano presenti proprio nei sistemi di collegamento in remoto rappresenta un fattore ulteriore di preoccupazione.

Condividi l'articolo

SkyArk: uno strumento open per individuare falle in AWS e Azure Allarme QSnatch: il malware ha colpito più di 60.000 NAS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/29/infrastrutture-critiche-a-rischio-il-bug-e-nelle-vpn/?utm_source=rss&utm_medium=rss&utm_campaign=infrastrutture-critiche-a-rischio-il-bug-e-nelle-vpn