

URGENT11: raffica di vulnerabilità in dispositivi SCADA e IoT

Lug 30, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le 11 falle di sicurezza interessano il software VxWorks. A rischio dispositivi medici, industriali e device IoT di ogni genere e tipo.

Si chiama **VxWorks** e , da un punto di vista tecnico, viene definito un “sistema operativo real-time” (RTOSes), cioè un software di controllo con funzionalità piuttosto limitate, installati normalmente sui chip che equipaggiano i dispositivi IoT o macchinari automatizzati.

Il fatto che sia pressoché sconosciuto al grande pubblico, non deve ingannare. Secondo quanto riporta il sito di **Wind River**, produttore del RTOSes, ci sarebbero infatti in circolazione la bellezza di 2 miliardi di dispositivi equipaggiati con VxWorks.

La notizia che un gruppo di ricercatori di **Armis** abbia individuato **11 falle di sicurezza** nel software (qui il documento che le riassume) di conseguenza, è più che sufficiente per mettere in fibrillazione l'intero settore della sicurezza.

Il fatto che i ricercatori abbiano battezzato il “pacchetto” di vulnerabilità con il nome di **URGENT11** la dice lunga sul possibile impatto che possono avere.

Tanto più che sei di queste (in questo caso abbiamo deciso di

lasciare la descrizione in inglese) sono state classificate “ad alto rischio”, dal momento che possono portare all’esecuzione di codice in remoto.

1. Stack overflow in the parsing of IPv4 packets IP options (CVE-2019-12256)
2. TCP Urgent Pointer = 0 leads to integer underflow (CVE-2019-12255)
3. TCP Urgent Pointer state confusion caused by malformed TCP A0 option (CVE-2019-12260)
4. TCP Urgent Pointer state confusion during connect to a remote host (CVE-2019-12261)
5. TCP Urgent Pointer state confusion due to race condition (CVE-2019-12263)
6. Heap overflow in DHCP Offer/ACK parsing in ipdhcpc (CVE-2019-12257)

Le altre cinque, considerate meno gravi, possono comunque essere sfruttate per provocare errori, malfunzionamenti e blocco dei sistemi.

1. TCP connection DoS via malformed TCP options (CVE-2019-12258)

2. Handling of unsolicited Reverse ARP replies (Logical Flaw) (CVE-2019-12262)
3. Logical flaw in IPv4 assignment by the ipdhcpc DHCP client (CVE-2019-12264)
4. DoS via NULL dereference in IGMP parsing (CVE-2019-12259)
5. IGMP Information leak via IGMPv3 specific membership report (CVE-2019-12265)

Considerato il tipo di dispositivi coinvolti, però, sottovalutare l'impatto di eventuali attacchi che sfruttino anche queste vulnerabilità "minori" sarebbe pericolosissimo. **Pensiamo ai danni che può provocare un blocco su una catena di montaggio o il malfunzionamento di un dispositivo medico.**

La nuova versione di VxWorks, con gli aggiornamenti che correggono le falle di sicurezza, è stata pubblicata dal produttore ed è disponibile dal mese scorso. Il problema, adesso, è capire come procederanno gli aggiornamenti.

Purtroppo l'esperienza porta a un certo pessimismo e non ci sono dubbi che sentiremo parlare di nuovo del sistema operativo real-time nel prossimo futuro.

Condividi l'articolo

Kaspersky supera l'audit indipendente SOC 2

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/07/30/urgent11-raffica-di-vulnerabilita-in-dispositivi-scada-e-iot/>