rittmeyer
BRUGG

Sicherheitslücke in Wind River VxWorks

Im VxWorks Real Time Operating System von Wind River wurden mehrere Schwachstellen entdeckt. Die schwerwiegendste davon ist die Möglichkeit, Remote einen Code ausführen zu können.

Um was geht es?

Im VxWorks Operating System (RTOS) von Wind River wurden mehrere Schwachstellen entdeckt. Die schwerwiegendste Schwachstelle ermöglicht die Ausführung von Remotecode. VxWorks RTOS wird von verschiedenen Geräten in SCADA-Systemen (wie Riflex M1 Steuerungen) von Industriesteuerungen eingesetzt. Eine erfolgreiche Ausnutzung dieser Schwachstelle kann dazu führen, dass ein entfernter Angreifer Zugriff auf ein Gerät erhält.

Betroffene Systeme:

- VxWorks 7 (SR540 und SR610)
- VxWorks 6.5-6.9
- Versionen von VxWorks mit dem Interpeak standalone network stack

Eine weitere Sicherheitslücke (als Ripple20 bekannt) kann sich auf die Treck IP-Stack-Implementierungen für eingebettete Systeme auswirken. Ein entfernter Angreifer kann einige dieser Schwachstellen ausnutzen und die Kontrolle eines Systems übernehmen.

Wie ist die Bedrohungslage auf meiner Anlage?

Die von Rittmeyer eingesetzten CPU's in den Riflex M1 Steuerungen laufen auf **VxWorks 5.4** und **5.5.1** und sind somit **nicht** betroffen. Auch von Ripple20 ist keines der von uns eingesetzten Systeme betroffen.

- Eine Stapelüberlaufschwachstelle besteht, wenn VxWorks v6.9.4 und höher IPv4-Optionen unsachgemäss parst (CVE-2019-12256)
- In VxWorks gibt es vier Sicherheitslücken durch Speicherverfälschung aufgrund unsachgemässer Handhabung des TCP-Feldes Urgent Point (CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263)
- Eine Heap-Überlauf-Schwachstelle besteht, wenn der DHCP-Client von VxWorks DHCP Offer/ACK-Pakete unsachgemäss parst. (CVE-2019-12257)
- Eine Denial-of-Service-Schwachstelle besteht, wenn VxWorks v6.5 und höher fehlerhafte TCP-Optionen unsachgemäss parst (CVE-2019-12258)
- Eine Denial-of-Service-Schwachstelle besteht, wenn VxWorks v6.5 und höher unsachgemäss Reverse-ARP-Antwortpakete parst (CVE-2019-12262)
- Eine Denial-of-Service-Schwachstelle besteht im integrierten DHCP-Client von VxWorks v6.5 und höher, der eine beliebige IP-Adresszuweisung akzeptiert (CVE-2019-12264)
- Es besteht eine Denial-of-Service-Schwachstelle, wenn VxWorks v6.5 und höher ein speziell gestaltetes DHCP-Antwortpaket empfängt, um die Zuweisung einer Multicast-Adresse zu erzwingen. Dies kann von einem IGMPv3-Mitgliedschaftsabfrage-Paket gefolgt werden, das zu einer NULL-Dereferenz im Netzwerk-Stack führt (CVE-2019-12259)

Wie kann ich mich dagegen schützen?

Mit der eingesetzten Software Version besteht bei Riflex M1 Steuerungen kein Handlungsbedarf.

Sollten Sie Steuerungen anderer Hersteller mit Versionen VxWorks 7 (SR540 und SR610) und VxWorks 6.5-6.9 im Einsatz haben, empfehlen wir Ihnen folgende Aktionen:

Installieren Sie die neuesten Patches, die von Wind River oder dem Produkthersteller bereitgestellt werden.
Führen Sie die gesamte Software als nicht privilegierter Benutzer (ohne Administratorrechte) aus, um die Auswirkungen eines erfolgreichen Angriffs zu verringern.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity