TCP / IP Dizinindeki Çoklu Güvenlik Açıklarının Etkisi (Ripple 20)

Yayın tarihi: 24 Eylül 2020

Mitsubishi Electric Corporation

Genel Bakış

TCP / IP Dizininde (Ripple20) 19 güvenlik açığı açıklandı. Bu güvenlik açıklarından kötü niyetli bir saldırgan tarafından yararlanılırsa, bilginin açığa çıkması, bilgilerin yok edilmesi veya tahrif edilmesi, hizmet reddi (DoS) ve uzaktan kod yürütme (RCE) gibi çeşitli riskler vardır. Bu güvenlik açıklarından bazıları birkaç ürünümüzü etkiliyor. Aşağıda, bu güvenlik açıklarından bazılarından etkilenen ürünlerin listesi verilmiştir, lütfen bu duruma karşı önlemler veya azaltıcı / geçici çözümler alınız. Ve bu güvenlik açıklarından bazılarından etkilenen ürünlerin adları ve ayrıca karşı önlemler ve azaltıcı / geçici çözümler birer birer güncellenecektir.

Açıklama

Treck IP Stack ve Zuken Elmic IP Stack'de (KASAGO ○ R) aşağıda listelenen 19 güvenlik açığı vardır. Ürünlerimiz de bazılarından etkilenebilir. **Lütfen "Etkilenen ürünler, karşı önlemler ve azaltıcı veya geçici çözümler" bölümündeki her ürünü etkileyebilecek güvenlik açığı sayılarını (aşağıda 1 - 19) kontrol ediniz.**

(1) IPv4 ve UDP bileşenlerinde Uzaktan Kod Yürütme güvenlik açığı (CVE-2020-11896)

(2) IPv6 bileşeninde Uzaktan Kod Yürütme güvenlik açığı (CVE- 020-11897)

(3) IPv4 ve ICMPv4 bileşenlerinde Bilgi Açıklama güvenlik açığı (CVE-2020-11898)

(4) IPv6 bileşenindeki (CVE-2020-11899) Bilgi İfşası ve Hizmet Reddi (DoS) güvenlik açıkları

(5) IPv4 tünel oluşturma bileşeninde (CVE-2020-11900) Hizmet Reddi (DoS) güvenlik açığı

(6) DNS çözümleyici bileşeninde Uzaktan Kod Yürütme güvenlik açığı (CVE-2020-11901)

(7) IPv4 tünel oluşturma bileşeni üzerinden IPv6'da Bilgi Açıklama güvenlik açığı (CVE -2020 -11902)

(8) DHCP bileşenindeki Bilgi Açığı güvenlik açığı (CVE-2020-11903)

(9) Bellek Ayırma bileşenindeki (CVE-2020-11904) Bilgi Bozulması, Hizmet Reddi (DoS) ve Uzaktan Kod Yürütme güvenlik açıkları

(10) DHCPv6 Bileşeninde (CVE-2020-11905) Bilgi Açığı güvenlik açığı

(11) Ethernet Bağlantı Katmanı bileşeninde (CVE-2020-11906) Hizmet Reddi (DoS) güvenlik açığı

(12) TCP bileşenlerinde Hizmet Reddi (DoS) güvenlik açığı (CVE-2020-11907)

(13) DHCP bileşenindeki Bilgi Açığı güvenlik açığı (CVE-2020-11908)

(14) IPv4 bileşeninde (CVE-2020-11909) Hizmet Reddi (DoS) güvenlik açığı

(15) ICMPv4 bileşenindeki Bilgi Açığı güvenlik açığı (CVE-2020-11910)

(16) ICMPv4 bileşeninde (CVE-2020-11911) Hizmet Reddi (DoS) güvenlik açığı

(17) TCP bileşenindeki Bilgi Açığı güvenlik açığı (CVE-2020-11912)

(18) IPv6 bileşenindeki Bilgi Açığı güvenlik açığı (CVE-2020-11913)

(19) ARP bileşeninde Bilgi Açığı güvenlik açığı (CVE-2020-11914)

Etki

Beklenen tehditler üründen ürüne değişir, ancak bu güvenlik açıklarından bir saldırgan tarafından yararlanılırsa, bilgilerin açığa çıkması, bilgilerin yok edilmesi veya tahrif edilmesi, hizmet reddi (DoS) ve uzaktan kod çalıştırma (RCE) gibi çeşitli etkileri vardır.

Etkilenen ürünler, karşı önlemler ve hafifletmeler veya geçici çözümler

[1] [Wi-Fi Arayüzü]

Model	Karşı Önlemler ve Azaltıcılar / Çözümler
MAC-557IF-E PAC-WF010-E MAC-558IF-E MAC-559IF-E PAC-WHS01WF-E (3, 6, 9, 12, 13,16,17, 19'dan etkilenebilir)	<Beklenen Etki> Bu güvenlik açıklarından kötü niyetli bir saldırgan tarafından yararlanılırsa, hizmet reddi (DoS), bilgilerin değiştirilmesi veya bilgilerin açığa çıkması gibi çeşitli etkiler olabilir. <Önlemler> Aşağıda önerilen azaltıcı veya geçici çözümler. <Azaltıcılar / Çözümler> 1. Yönlendirici ayarlarının aşağıdaki gibi olup olmadığını kontrol edin. 1-1. Kablosuz LAN'ın tanımlanabilen şifresini kolay tespit edilemeyecek şekilde ayarlayınız. Şifre ilk kurulumda değiştirilecek ise, ardışık sayılardan ve tahmin edilebilir MAC adresinden kaçınınız ve harfleri, sayıları karıştırarak bir şifre belirleyiniz. 1-2. WEP şifreleme algoritması veya Açık kimlik doğrulama kullanmayınız. 1-3. Yönlendirici ayarlarını değiştirirseniz, yetkisiz erişimi zorlaştırmak için internetteki görünürlüğünü gizleyiniz. (ör. PING isteğine yanıt vermeyecek şekilde ayarlayınız) 1-4. Yönlendiricinin, yönetici portalı için tanımlanması zor olan şifre belirleyiniz. 2. Evde bilgisayar veya tablet vb. Kullanırken aşağıdakileri kontrol ediniz. 2-1. Antivirüs yazılımını en son sürüme güncelleyiniz. 2-2. Şüpheli ek dosyasını veya bağlantılı URL'yi açmayınız veya bunlara erişmeyiniz.

* İletişim bilgileri

Lütfen yerel Mitsubishi Electric temsilcinizle iletişime geçiniz.

İletişim bilgileri (Yalnızca yukarıdakilerin dışındaki ürünler için)

https://www.mitsubishielectric.com/contact/ssl/php/1334/kiyaku.php?fid=1334&Vul=Ripple20

Referanslar

- CERT / CC Güvenlik Açığı Notu "VU # 257161 Treck IP yığınları birden fazla güvenlik açığı içerir"

https://www.kb.cert.org/vuls/id/257161

- ICS Danışmanlığı "ICSA-20-168-01 Treck TCP / IP Yığını"

https://www.us-cert.gov/ics/advisories/icsa-20-168-01

- JSOF "Ripple20"

https://www.jsof-tech.com/ripple20/

- Treck Inc. "Güvenlik Açığı Yanıt Bilgileri"

https://treck.com/vulnerability-response-information/