2020 年 6 月 24 日

多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報

2020 年 6 月 16 日、米国国土安全保障省(DHS)の ICS-CERT は、TCP/IP ライブラリの脆弱性「Ripple20」に関するアドバイザリを発行し、2020 年 6 月 18 日、内閣サイバーセキュリティセンターは、重要インフラ事業者等に向けて情報提供を行いました。

本脆弱性の影響は、ネットワーク製品に組み込まれているライブラリに関するものであり、範囲が広い反面、特定、対応が容易でないことから、一般に公開するものです。

資料　多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報

本件に関する連絡先
内閣サイバーセキュリティセンター
電話番号　03-5253-2111（代表）
　重要インフラ第２グループ

資料

2020 年 6 月 18 日

内閣サイバーセキュリティセンター
重要インフラグループ

多くのデバイスが影響を受ける複数の脆弱性「Ripple20」に関する参考情報

2020 年 6 月 16 日、ICS-CERT は、多くのデバイスが影響を受ける TCP/IP ライブラリに関する 19 個の脆弱性「Ripple20」のアドバイザリを発行しました。本参考情報を確認し、「Ripple20」の概要を把握するとともに必要な対応を検討してください。

1. 概要

2020 年 6 月 16 日、ICS-CERT は、多くのデバイス（例.産業用制御機器、スマートデバイス、UPS、ルーター、プリンター、医療機器等）が影響を受ける複数の脆弱性「Ripple20」に関するアドバイザリを発行しました。ICS-CERT によると、「Ripple20」は、TCP/IP ライブラリ[1]に存在する 19 個の脆弱性の総称であり、本ライブラリを使用しているネットワークを使用する製品に本脆弱性の影響を受ける可能性があるとしています。

本脆弱性に対して、既に脆弱性パッチが一部公表されているものの、ほとんどの製品で修正されていないのが現状です。「Ripple20」の影響を受けるライブラリは、Treck 社とエルミックシステムズ社(現在は、図研エルミック社)が開発したものとしており、「Treck TCP/IP」や「KASAGO 製品」として、種々のデバイスに組み込まれています。これらのライブラリは、基礎的なものであることから、サプライチェーンの特性上、脆弱性を含む製品の特定は容易ではありません。

「Ripple20」が悪用された場合、リモートで特別に細工したネットワークパケットを使用して、サービス拒否が引き起こされたり、情報が開示されたり、任意のコードが実行される可能性があります。

[1] 汎用性が高い特定の機能を持つプログラムを再利用可能な形でまとめたもの。

ICS-CERT によれば、「Ripple20」に含まれる 19 個の脆弱性を脆弱性の共通評価手法 CVSSv3 で評価した結果を表 1 に示します。詳細は、参考 URL に記載した ICS-CERT のアドバイザリを参照してください。

表 1　「Ripple20」に含まれる 19 個の脆弱性に対する CVSSv3 評価結果

No	脆弱性(CVE 番号)	CVSSv3 基本値[2]
1	CVE-2020-11896	10.0
2	CVE-2020-11897	10.0
3	CVE-2020-11898	9.1
4	CVE-2020-11899	5.4
5	CVE-2020-11900	8.2
6	CVE-2020-11901	9.0
7	CVE-2020-11902	7.3
8	CVE-2020-11903	5.3
9	CVE-2020-11904	5.6
10	CVE-2020-11905	5.3
11	CVE-2020-11906	5.0
12	CVE-2020-11907	5.0
13	CVE-2020-11908	3.1
14	CVE-2020-11909	3.7
15	CVE-2020-11910	3.7
16	CVE-2020-11911	3.7
17	CVE-2020-11912	3.7
18	CVE-2020-11913	3.7
19	CVE-2020-11914	3.1

2. 対象製品

- 「Treck TCP/IP stack」を使用している製品
- 「KASAGO IPv4 Light」、「KASAGO IPv4」、「KASAGO IPv6/v4 Dual」、「KASAGO DHCPv6」を使用している製品

3. 対応

各重要インフラ事業者等の CISO においては、本脆弱性を把握し、自組織における対応（緩和策、抜本的対策、万一の場合の対応を含む）について、検討を行うことを推奨します。

[2] 脆弱性の共通評価手法。攻撃の難易度や攻撃による影響をもとに、脆弱性を評価する。深刻度を 5 段階でレベル分けし、10.0～9.0 を「緊急」、8.9～7.0 を「重要」、6.9～4.0 を「警告」、3.9～0.1 を「注意」、0 を「なし」と分類。表では、ICS-CERT のアドバイザリに掲載されている評価値を記載。

ICS-CERT は、2020 年 6 月 17 日付けのアドバイザリの中で、以下の緩和策等を推奨しています。

- 産業用制御機器やシステムのネットワークへの露出を必要最小限に抑え、インターネットからアクセスできないようにする。
- 制御システムのネットワークとデバイスをファイアウォールの後方に配置し、事務作業等を行う情報系ネットワークから分離する。

参考 URL

- ICS Advisory (ICSA-20-168-01) -Treck TCP/IP Stack- (ICS-CERT)
  https://www.us-cert.gov/ics/advisories/icsa-20-168-01
- Ripple20 -19 Zero-Day Vulnerabilities Amplified by the Supply Chain- (JSOF)
  https://www.jsof-tech.com/ripple20/
- Treck IP stacks contain multiple vulnerabilities
  Vulnerability Note VU#257161 (CERT/CC)
  https://kb.cert.org/vuls/id/257161
- Vulnerability Response Information (Treck)
  https://treck.com/vulnerability-response-information/
- KASAGO 製品における脆弱性に関するお知らせ（図研エルミック）
  https://www.elwsc.co.jp/wp-content/uploads/2020/06/KASAGO202006-1.pdf
- HPSBPI03666 rev. 1 - Certain HP and Samsung-branded Print Products - Network Stack Potential Vulnerabilities (HP)
  https://support.hp.com/us-en/document/c06640149
- 2020.1 IPU - Intel(r) CSME, SPS, TXE, AMT, ISM and DAL Advisory (Intel)
  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html