

BD Product Name: BD Rowa™ Label Printer

Date of Security Patches: October 2020

Abstract: Treck Inc. – Recommend Product Security Patches – October 2020

Microsoft® & Third-Party Patches

BD™ has identified patches from Treck Inc. that address critical, high and medium severity vulnerabilities previously reported to exist in Treck's TCP/IPv4/v6 and associated protocols. Patches for affected products have been published [via the vendor's website](#) effective September 2020. These patches were not found to adversely affect BD Rowa™ products. Patches will be applied according to customers' service agreement.

Customers that maintain patches independent of BD™ automated delivery should ensure the validated patches are installed on their BD Rowa™ systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Patch Name	Patch Description	Patch ID	Notes
Treck Inc.– Critical Severity Patch: CVE-2020-11896	Resolves the Treck TCP/IP vulnerability that allows Remote Code Execution in the IPv4 tunneling stack that affects versions before v6.0.1.66	TRECK-CVE-2020-11896	1
Treck Inc.– Critical Severity Patch: CVE-2020-11897	Resolves the Treck TCP/IP vulnerability that has an Out-of-Bounds Write via multiple malformed IPv6 packets that affects versions before v5.0.1.35	TRECK-CVE-2020-11897	1
Treck Inc.– Critical Severity Patch: CVE-2020-11898	Resolves the Treck TCP/IP vulnerability that improperly handles an IPv4/ICMPv4 Length Parameter Inconsistency, which might allow remote attackers to trigger an information leak that affects versions before v6.0.1.66	TRECK-CVE-2020-11898	1
Treck Inc. – Critical Severity Patch: CVE-2020-11901	Resolves the Treck TCP/IP vulnerability that allows Remote Code execution via a single invalid DNS response that affects versions before v6.0.1.66	TRECK-CVE-2020-11901	1
Treck Inc. - Critical Severity Patch: CVE-2020-11906	Resolves the Treck TCP/IP vulnerability that permits an Ethernet Link Layer Integer Underflow that affects versions before v6.0.1.66	TRECK-CVE-2020-11906	1
Treck Inc.– High Severity Patch: CVE-2020-11900	Resolves the Treck TCP/IP vulnerability that permits an IPv4 tunneling Double Free that affects versions before v6.0.1.41	TRECK-CVE-2020-11900	1
Treck Inc. – High Severity Patch: CVE-2020-11902	Resolves the Treck TCP/IP vulnerability that permits an IPv6OverIPv4 tunneling Out-of-bounds Read that affects versions before v6.0.1.66	TRECK-CVE-2020-11902	1
Treck Inc. – High Severity Patch: CVE-2020-11904	Resolves the Treck TCP/IP vulnerability that permits an Integer Overflow during Memory Allocation that causes an Out-of-Bounds Write affecting versions before v6.0.1.66	TRECK-CVE-2020-11904	1
Treck Inc. - Medium Severity Patch: CVE-2020-11903	Resolves the Treck TCP/IP vulnerability that permits a DHCP Out-of-bounds Read that affects versions before v6.0.1.28	TRECK-CVE-2020-11903	1
Treck Inc. – Medium Severity Patch: CVE-2020-11905	Resolves the Treck TCP/IP vulnerability that permits a DHCPv6 Out-of-bounds Read that affects versions before v6.0.1.66	TRECK-CVE-2020-11905	1
Treck Inc.– Medium Severity Patch: CVE-2020-11899	Resolves the Treck TCP/IP vulnerability that has an Out-of-Bounds Read via multiple malformed IPv6 packets that affects versions before v6.0.1.66	TRECK-CVE-2020-11899	1



Treck Inc. – Medium Severity Patch: CVE-2020-11907	Resolves the Treck TCP/IP vulnerability that improperly handles a Length Parameter Inconsistency in TCP that affects versions before v6.0.1.66	<u>TRECK-CVE-2020-11907</u>	1
---	--	-----------------------------	---

Notes

1. For customers using BD Rowa™ Label Printer Technology impacted by this vulnerability, please contact your BD Rowa regional Customer Support Center to assist identifying and installation of the correct patch(es) that applies to your BD Rowa product. Patches may require the system to reboot.

