

02 June 2020  
300480415/pbsa56

## Security Advisory for FL MGUARD, TC MGUARD, TC ROUTER and TC CLOUD CLIENT devices

### Advisory Title

A critical vulnerability has been discovered in PPPD which is utilized in Phoenix Contact FL MGUARD, TC MGUARD, TC ROUTER and TC CLOUD CLIENT devices.

### Advisory ID

CVE-2020-8597  
VDE-2020-018

### Vulnerability Description

FL MGUARD, TC MGUARD, TC ROUTER and TC CLOUD CLIENT devices are affected by a buffer overflow vulnerability within the PPP service.

The PPP service is not active by default, but is used commonly at TC ROUTER, TC CLOUD CLIENT.

It is also running in the following FL MGUARD and TC MGUARD configurations:

- Mobile data connection
- Router mode "Modem"
- Router mode "PPPoE"
- L2TP over IPsec

Malicious PPP peers could try to exploit the vulnerability from remote.

**Affected products**

Article no	Article	Affected versions	Current version
2200515	FL MGUARD RS4000 TX/TX VPN	< 8.8.2	<a href="#">download</a>
2700197	FL MGUARD GT/GT	< 8.8.2	<a href="#">download</a>
2700198	FL MGUARD GT/GT VPN	< 8.8.2	<a href="#">download</a>
2700634	FL MGUARD RS4000 TX/TX	< 8.8.2	<a href="#">download</a>
2700639	FL MGUARD SMART2 VPN	< 8.8.2	<a href="#">download</a>
2700640	FL MGUARD SMART2	< 8.8.2	<a href="#">download</a>
2700642	FL MGUARD RS2000 TX/TX VPN	< 8.8.2	<a href="#">download</a>
2700967	FL MGUARD DELTA TX/TX	< 8.8.2	<a href="#">download</a>
2700968	FL MGUARD DELTA TX/TX VPN	< 8.8.2	<a href="#">download</a>
2701275	FL MGUARD PCI4000 VPN	< 8.8.2	<a href="#">download</a>
2701278	FL MGUARD PCIE4000 VPN	< 8.8.2	<a href="#">download</a>
2701875	FL MGUARD RS2005 TX VPN	< 8.8.2	<a href="#">download</a>
2701876	FL MGUARD RS4004 TX/DTX	< 8.8.2	<a href="#">download</a>
2701877	FL MGUARD RS4004 TX/DTX VPN	< 8.8.2	<a href="#">download</a>
2702259	FL MGUARD RS4000 TX/TX-P	< 8.8.2	<a href="#">download</a>
2702465	FL MGUARD RS4000 TX/TX VPN-M	< 8.8.2	<a href="#">download</a>
2702547	FL MGUARD CENTERPORT	< 8.8.2	<a href="#">download</a>
2702831	FL MGUARD CORE TX VPN	< 8.8.2	<a href="#">download</a>
2702139	FL MGUARD RS2000 TX/TX-B	< 8.8.2	<a href="#">download</a>
1053405	FL MGUARD SMART2 VPN/K1	< 8.8.2	<a href="#">download</a>
1053403	FL MGUARD RS4000 TX/TX VPN/K1	< 8.8.2	<a href="#">download</a>
1073940	FL MGUARD PCIE4000 VPN/K2	< 8.8.2	<a href="#">download</a>
1073943	FL MGUARD RS4000 VPN/K2	< 8.8.2	<a href="#">download</a>
1073944	FL MGUARD PCI4000 VPN/K2	< 8.8.2	<a href="#">download</a>
2903441	TC MGUARD RS2000 3G VPN	< 8.8.2	<a href="#">download</a>
2903588	TC MGUARD RS2000 4G VPN	< 8.8.2	<a href="#">download</a>
1010462	TC MGUARD RS2000 4G VZW VPN	< 8.8.2	<a href="#">download</a>
1010464	TC MGUARD RS2000 4G ATT VPN	< 8.8.2	<a href="#">download</a>
2903440	TC MGUARD RS4000 3G VPN	< 8.8.2	<a href="#">download</a>
2903586	TC MGUARD RS4000 4G VPN	< 8.8.2	<a href="#">download</a>
1010461	TC MGUARD RS4000 4G VZW VPN	< 8.8.2	<a href="#">download</a>
1010463	TC MGUARD RS4000 4G ATT VPN	< 8.8.2	<a href="#">download</a>
2702528	TC ROUTER 3002T-4G	< 2.05.5	<a href="#">download</a>

2702530	TC ROUTER 3002T-4G	< 2.05.5	<a href="#">download</a>
2702529	TC ROUTER 2002T-3G	< 2.05.5	<a href="#">download</a>
2702531	TC ROUTER 2002T-3G	< 2.05.5	<a href="#">download</a>
2702532	TC ROUTER 3002T-4G VZW	< 2.05.5	<a href="#">download</a>
2702533	TC ROUTER 3002T-4G ATT	< 2.05.5	<a href="#">download</a>
2702886	TC CLOUD CLIENT 1002-4G	< 2.03.19	<a href="#">download</a>
2702887	TC CLOUD CLIENT 1002-4G VZW	< 2.03.19	<a href="#">download</a>
2702888	TC CLOUD CLIENT 1002-4G ATT	< 2.03.19	<a href="#">download</a>

And all Innominate derivatives of FL MGUARD products.

### **Impact**

Attackers may either crash the PPP service or execute code with system permissions.

### **Classification of Vulnerability**

Base Score: 9.8

CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

At TC ROUTER and TC CLOUD CLIENT devices PPPD is not started by default but is activated as soon as packet data is enabled in the packet data setup.

The FL MGUARD and TC MGUARD is vulnerable only in certain configurations, listed under vulnerability description. Within these configurations, the MGUARD acts as PPP client, which establishes connections to remote peers.

### **Remediation**

We strongly recommend updating the devices to the latest firmware as listed in the table above if the devices are used in configurations where PPPD is activated.