TLP:WHITE

VDE-2024-052: Phoenix Contact: Multiple mGuard devices are vulnerable to a drain of open file descriptors.

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Sep 10 12:00:00 CEST 2024	Engine: 2.5.11
Current release date: Tue Sep 10 12:00:00 CEST 2024	Build Date: Thu Aug 29 10:55:06 CEST 2024
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 5.3	Severity: medium
Original language:	Language: en-US
Also referred to: VDE-2024-052, PCSA-2024/00010	

Summary

The pathfinder TCP encapsulation service is vulnerable to a drain of open file descriptors.

General Recommendation

For general information and recommendations on security measures refer to the mGuard documentation: https://help.mguard.com/en/documentation

Impact

Attackers can trigger a denial-of-service of the pathfinder TCP encapsulation service.

Mitigation

Access to the listen port of the pathfinder TCP encapsulation service should be limited to trustworthy networks or peers.

Remediation

Phoenix Contact strongly recommends upgrading affected mGuard devices to firmware version 8.9.3 / 10.4.1 or higher which fixes this vulnerability.

Product Description

mGuards are industrial routers and security appliances

Summary

The pathfinder TCP encapsulation service is vulnerable to a drain of open file descriptors.

Product groups

Affected Products.

- Firmware < 8.9.3 installed on FL MGUARD RS2000 TX/TX VPN
- Firmware < 8.9.3 installed on FL MGUARD RS2005 TX VPN
- Firmware < 8.9.3 installed on TC MGUARD RS2000 3G VPN
- Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX
- Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX VPN
- Firmware < 8.9.3 installed on FL MGUARD RS4004 TX/DTX
- Firmware < 8.9.3 installed on FL MGUARD RS4004 TX/DTX VPN
- Firmware < 8.9.3 installed on TC MGUARD RS4000 3G VPN
- Firmware < 8.9.3 installed on FL MGUARD RS2000 TX/TX-B
- Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX-P
- Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX-M
- Firmware < 8.9.3 installed on FL MGUARD PCI4000
- Firmware < 8.9.3 installed on FL MGUARD PCI4000 VPN
- Firmware < 8.9.3 installed on FL MGUARD PCIE4000
- Firmware < 8.9.3 installed on FL MGUARD PCIE4000 VPN
- Firmware < 8.9.3 installed on FL MGUARD DELTA TX/TX
- Firmware < 8.9.3 installed on FL MGUARD DELTA TX/TX VPN
- Firmware < 8.9.3 installed on FL MGUARD SMART2
- Firmware < 8.9.3 installed on FL MGUARD SMART2 VPN
- Firmware < 8.9.3 installed on FL MGUARD CORE TX
- Firmware < 8.9.3 installed on FL MGUARD CORE TX VPN
- Firmware < 8.9.3 installed on TC MGUARD RS2000 4G VPN
- Firmware < 8.9.3 installed on TC MGUARD RS4000 4G VPN
- Firmware < 8.9.3 installed on TC MGUARD RS4000 4G VZW VPN
- Firmware < 8.9.3 installed on TC MGUARD RS2000 4G VZW VPN
- Firmware < 8.9.3 installed on TC MGUARD RS4000 4G ATT VPN
- Firmware < 8.9.3 installed on TC MGUARD RS2000 4G ATT VPN
- Firmware < 8.9.3 installed on FL MGUARD GT/GT
- Firmware < 8.9.3 installed on FL MGUARD GT/GT VPN
- Firmware < 8.9.3 installed on FL MGUARD CENTERPORT
- Firmware < 8.9.3 installed on FL MGUARD CENTERPORT VPN-1000
- Firmware < 10.4.1 installed on FL MGUARD 2102
- Firmware < 10.4.1 installed on FL MGUARD 2105
- Firmware < 10.4.1 installed on FL MGUARD 4302
- Firmware < 10.4.1 installed on FL MGUARD 4305
- Firmware < 10.4.1 installed on FL MGUARD 4102 PCIE
- Firmware < 10.4.1 installed on FL MGUARD 4102 PCI

Fixed Products.

- Firmware 8.9.3 installed on FL MGUARD RS2000 TX/TX VPN
- Firmware 8.9.3 installed on FL MGUARD RS2005 TX VPN
- Firmware 8.9.3 installed on TC MGUARD RS2000 3G VPN
- Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX
- Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX VPN
- Firmware 8.9.3 installed on FL MGUARD RS4004 TX/DTX
- Firmware 8.9.3 installed on FL MGUARD RS4004 TX/DTX VPN
- Firmware 8.9.3 installed on TC MGUARD RS4000 3G VPN
- Firmware 8.9.3 installed on FL MGUARD RS2000 TX/TX-B
- Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX-P
- Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX-M
- Firmware 8.9.3 installed on FL MGUARD PCI4000
- Firmware 8.9.3 installed on FL MGUARD PCI4000 VPN
- Firmware 8.9.3 installed on FL MGUARD PCIE4000
- Firmware 8.9.3 installed on FL MGUARD PCIE4000 VPN
- Firmware 8.9.3 installed on FL MGUARD DELTA TX/TX
- Firmware 8.9.3 installed on FL MGUARD DELTA TX/TX VPN
- Firmware 8.9.3 installed on FL MGUARD SMART2
- Firmware 8.9.3 installed on FL MGUARD SMART2 VPN
- Firmware 8.9.3 installed on FL MGUARD CORE TX
- Firmware 8.9.3 installed on FL MGUARD CORE TX VPN
- Firmware 8.9.3 installed on TC MGUARD RS2000 4G VPN
- Firmware 8.9.3 installed on TC MGUARD RS4000 4G VPN
- Firmware 8.9.3 installed on TC MGUARD RS4000 4G VZW VPN
- Firmware 8.9.3 installed on TC MGUARD RS2000 4G VZW VPN
- Firmware 8.9.3 installed on TC MGUARD RS4000 4G ATT VPN
- Firmware 8.9.3 installed on TC MGUARD RS2000 4G ATT VPN
- Firmware 8.9.3 installed on FL MGUARD GT/GT
- Firmware 8.9.3 installed on FL MGUARD GT/GT VPN
- Firmware 8.9.3 installed on FL MGUARD CENTERPORT
- Firmware 8.9.3 installed on FL MGUARD CENTERPORT VPN-1000
- Firmware 10.4.1 installed on FL MGUARD 2102
- Firmware 10.4.1 installed on FL MGUARD 2105
- Firmware 10.4.1 installed on FL MGUARD 4302
- Firmware 10.4.1 installed on FL MGUARD 4305
- Firmware 10.4.1 installed on FL MGUARD 4102 PCIE
- Firmware 10.4.1 installed on FL MGUARD 4102 PCI

Vulnerabilities

CVE-2024-7734 (CVE-2024-7734)

Vulnerability Description (all)

An unauthenticated remote attacker can exploit the behavior of the pathfinder TCP encapsulation service by establishing a high number of TCP connections to the pathfinder TCP encapsulation service. The impact is limited to blocking of valid IPsec VPN peers.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 8.9.3 installed on FL MGUARD RS2000 TX/TX VPN Order number: 2700642	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS2005 TX VPN Order number: 2701875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS2000 3G VPN Order number: 2903441	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX Order number: 2700634	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX VPN Order number: 2200515	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4004 TX/DTX Order number: 2701876	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4004 TX/DTX VPN Order number: 2701877	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS4000 3G VPN Order number: 2903440	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS2000 TX/TX-B Order number: 2702139	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX-P Order number: 2702259	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD RS4000 TX/TX-M Order number: 2702470	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD PCI4000 Order number: 2701274	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD PCI4000 VPN Order number: 2701275	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD PCIE4000 Order number: 2701277	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD PCIE4000 VPN Order number: 2701278	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD DELTA TX/TX Order number: 2700967	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD DELTA TX/TX VPN Order number: 2700968	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD SMART2 Order number: 2700640	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD SMART2 VPN Order number: 2700639	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD CORE TX Order number: 2702884	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD CORE TX VPN Order number: 2702831	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS2000 4G VPN Order number: 2903588	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS4000 4G VPN Order number: 2903586	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS4000 4G VZW VPN Order number: 1010461	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS2000 4G VZW VPN Order number: 1010462	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on TC MGUARD RS4000 4G ATT VPN Order number: 1010463	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Firmware < 8.9.3 installed on TC MGUARD RS2000 4G ATT VPN Order number: 1010464	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD GT/GT Order number: 2700197	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD GT/GT VPN Order number: 2700198	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD CENTERPORT Order number: 2702547	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 8.9.3 installed on FL MGUARD CENTERPORT VPN-1000 Order number: 2702820	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 2102 Order number: 1357828	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 2105 Order number: 1357850	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 4302 Order number: 1357840	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 4305 Order number: 1357875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 4102 PCIE Order number: 1357842	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
Firmware < 10.4.1 installed on FL MGUARD 4102 PCI Order number: 1441187	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
Firmware 8.9.3 installed on FL MGUARD RS2000 TX/TX VPN Order number: 2700642 (Download)
Firmware 8.9.3 installed on FL MGUARD RS2005 TX VPN Order number: 2701875 (Download)
Firmware 8.9.3 installed on TC MGUARD RS2000 3G VPN Order number: 2903441 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX Order number: 2700634 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX VPN Order number: 2200515 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4004 TX/DTX Order number: 2701876 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4004 TX/DTX VPN Order number: 2701877 (Download)
Firmware 8.9.3 installed on TC MGUARD RS4000 3G VPN Order number: 2903440 (Download)
Firmware 8.9.3 installed on FL MGUARD RS2000 TX/TX-B Order number: 2702139 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX-P Order number: 2702259 (Download)
Firmware 8.9.3 installed on FL MGUARD RS4000 TX/TX-M Order number: 2702470 (Download)
Firmware 8.9.3 installed on FL MGUARD PCI4000 Order number: 2701274 (Download)
Firmware 8.9.3 installed on FL MGUARD PCI4000 VPN Order number: 2701275 (Download)
Firmware 8.9.3 installed on FL MGUARD PCIE4000 Order number: 2701277 (Download)
Firmware 8.9.3 installed on FL MGUARD PCIE4000 VPN Order number: 2701278 (Download)
Firmware 8.9.3 installed on FL MGUARD DELTA TX/TX Order number: 2700967 (Download)

Firmware 8.9.3 installed on FL MGUARD DELTA TX/TX VPN Order number: 2700968 (Download)
Firmware 8.9.3 installed on FL MGUARD SMART2 Order number: 2700640 (Download)
Firmware 8.9.3 installed on FL MGUARD SMART2 VPN Order number: 2700639 (Download)
Firmware 8.9.3 installed on FL MGUARD CORE TX Order number: 2702884 (Download)
Firmware 8.9.3 installed on FL MGUARD CORE TX VPN Order number: 2702831 (Download)
Firmware 8.9.3 installed on TC MGUARD RS2000 4G VPN Order number: 2903588 (Download)
Firmware 8.9.3 installed on TC MGUARD RS4000 4G VPN Order number: 2903586 (Download)
Firmware 8.9.3 installed on TC MGUARD RS4000 4G VZW VPN Order number: 1010461 (Download)
Firmware 8.9.3 installed on TC MGUARD RS2000 4G VZW VPN Order number: 1010462 (Download)
Firmware 8.9.3 installed on TC MGUARD RS4000 4G ATT VPN Order number: 1010463 (Download)
Firmware 8.9.3 installed on TC MGUARD RS2000 4G ATT VPN Order number: 1010464 (Download)
Firmware 8.9.3 installed on FL MGUARD GT/GT Order number: 2700197 (Download)
Firmware 8.9.3 installed on FL MGUARD GT/GT VPN Order number: 2700198 (Download)
Firmware 8.9.3 installed on FL MGUARD CENTERPORT Order number: 2702547 (Download)
Firmware 8.9.3 installed on FL MGUARD CENTERPORT VPN-1000 Order number: 2702820 (Download)
Firmware 10.4.1 installed on FL MGUARD 2102 Order number: 1357828 (Download)
Firmware 10.4.1 installed on FL MGUARD 2105 Order number: 1357850 (Download)
Firmware 10.4.1 installed on FL MGUARD 4302 Order number: 1357840 (Download)
Firmware 10.4.1 installed on FL MGUARD 4305 Order number: 1357875 (Download)
Firmware 10.4.1 installed on FL MGUARD 4102 PCIE Order number: 1357842 (Download)
Firmware 10.4.1 installed on FL MGUARD 4102 PCI Order number: 1441187 (Download)

Remediations

Vendor fix

Phoenix Contact strongly recommends upgrading affected mGuard devices to firmware version 8.9.3 / 10.4.1 or higher which fixes this vulnerability.

For groups:

- Affected Products.

Mitigation

If possible, access to the listen port of the pathfinder TCP encapsulation service should be limited to trustworthy networks or peers.

For groups:

- Affected Products.

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination (see: https://certvde.com)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2024/00010: mGuard firmware < 8.9.3 / 10.4.1 is vulnerable to a drain of open file descriptors. (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact PSIRT (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://cert.vde.com/de/advisories/vendor/phoenixcontact/
- VDE-2024-052: Phoenix Contact: Multiple mGuard devices are vulnerable to a drain of open file descriptors. (SELF): https://cert.vde.com/en/advisories/VDE-2024-052

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Sep 10 12:00:00 CEST 2024	Initial revision.

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/