Galleon NTS-6002-GPS Command Injection

Helm
20 May 2022

TL;DR

Galleon Systems' GPS NTP time server had a command injection vulnerability in the firmware of their NTS GPS device which could allow total control of the device through the web management interface.

The vulnerability – CVE-2022-27224

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27224

- Device: Galleon NTS-6002-GPS

Categories

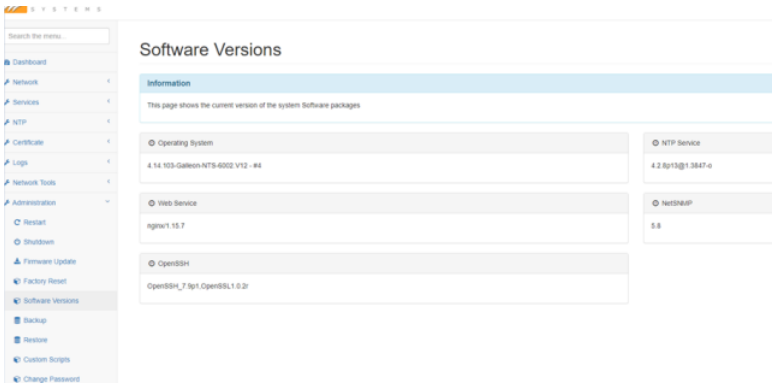
Show all

See the other cool stuff we've been doing...

DFIR
Hive Ransomware is on the rise. How should you deal with it?
18 NOV 2022

INTERNET OF THINGS
Effecting positive change in the Internet

SOCIAL ENGINEERING
Social Engineering dos and don'ts
20 OCT 2022



Moto E20 Readback Vulnerability
19 OCT 2022

MS Enterprise app management service RCE. CVE-2022-35841
13 OCT 2022

Summary

A vulnerability was discovered in Galleon NTS-6002-GPS 4.14.103-Galleon-NTS-6002.V12 #4. A low privilege authenticated attacker can perform command injection as the root user, by supplying shell metacharacters to forms on the Network Tools section of the web-management interface. All three networking tools are affected (Ping, Traceroute, and DNS Lookup) and their respective input fields (ping_address, trace_address, nslookup_address).

In the examples below, we are targeting one of the three vulnerable pages (in this case DNS Lookup). The vulnerable endpoint is “/tools/dolookup” and the parameter “nslookup_address”.

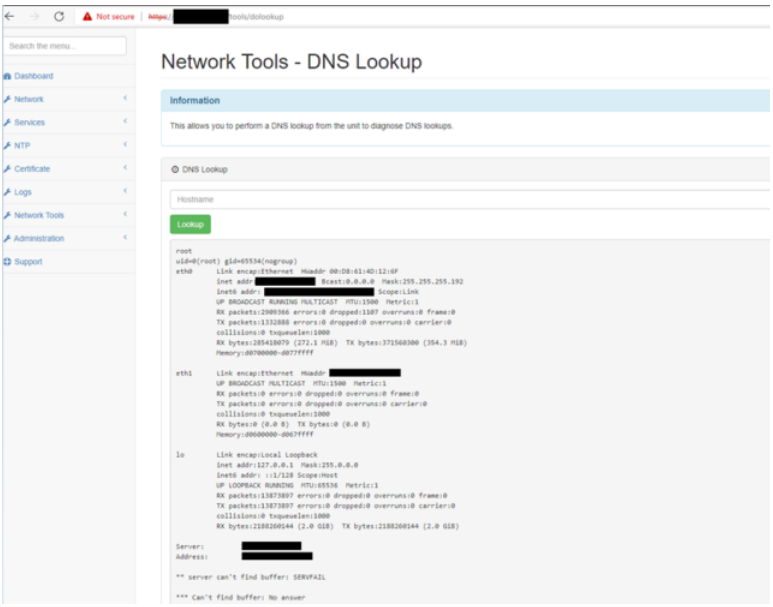
Example commands used to enumerate and perform command injection via the pages and injectable page parameters mentioned above (“buffer” is a chosen random input word expected by the application):

SERVICES
Penetration Testing

Find out more »

Our People

```
buffer&id&pwd&ls;
```



Exploitation

The underlying system did not allow some characters to be passed, these can be worked around using shell facilities. We can avoid the use of spaces by using the IFS shell variable (Input Field Separator):

```
buffer&cat${IFS}index.php
```

is über technical, but faceless relationships do nobody any good.
Meet the team »

Forward slashes "/" were also not accepted. In bash these can be replicated by using variable substitution, such as ${HOME:0:1}. This extracts the first character for the HOME shell variables, which, as the variable is a full path, is equal to the "/" character. With these substitutions we can submit most shell commands, such as:

```
buffer&cat${IFS}${HOME:0:1}etc${HOME:0:1}passwd
```

```
buffer&cat${IFS}${HOME:0:1}etc${HOME:0:1}shadow
```

The final command injection string gets the local Un*x system's password hash file. This is only accessible with "root" level privileges on the device, and therefore highlights another issue of the web management UI server being run via the "root" administrative account rather than a more sensible choice such as "www-var" or "apache".

Disclosure timeline

- Nov 21 – Initial disclosure to Galleon Systems
- Jan 22 – Acceptance of part of the vulnerability
- Jan 22 – Vendor started the vulnerability registration (CVE ID request dropped by MITRE due to failure by Galleon to provide additional information)
- Mar 22 – I disclosed the vulnerability to MITRE myself
- May 22 – MITRE acknowledged the vulnerability – CVE ID provided

Background

I found the vulnerability almost accidentally while doing other work. Wanting a change of focus I explored the web admin UI looking for basic vulnerabilities. Much to my surprise I found this device to be vulnerable.

Realistic impact

Command injection on a GPS powered NTP device could in theory be quite devastating. Once “root” level privileged command execution is gained on the device, an attacker could gain control over the network time which could interfere with the Kerberos authentication protocol. This would be compounded if no backup NTP source is available.

Mitigations

At the time of writing the vendor was working on releasing a newer iteration of the device's software which would patch the identified security issues. However it has not yet been released, and to the best our knowledge the update has not been tested or verified.

- While waiting for a vendor software patch, these devices should be properly restricted with firewalls at a host and / or network level in a manner that would only allow for IT management devices to authenticate to the device.
- Further, ensure the device is making use of a suitably complex and unique password so that an attacker could not trivially guess the password to the device's web admin UI.
- Ensure that more than one high tier NTP source is used to provide time for the network.

Disclosure challenges

The vendor attempted to deny that the webserver was running with "root" privileges. Here's what they said to us:

This had us falling about laughing!

Furthermore, as seen in the screenshots above, it was possible to retrieve the “/etc/shadow” hash file that is typically only accessible by the “root” account or an account with delegated “root” privileges (e.g SUID).

References

- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27224