SSD ADVISORY – HONGDIAN H8922 MULTIPLE VULNERABILITIES

April 24, 2021 SSD Secure Disclosure technical team
Vulnerability publication

TL;DR

Find out how multiple vulnerabilities in Hongdian H8922 allow an attacker to run arbitrary commands on the device with root privileges as well as access the device with root privileges via a backdoor account.

Vulnerability Summary

The H8922 "4G industrial router is based on 3G/4G wireless network and adopts a high-performance 32-bit embedded operating system with full industrial design. It supports wired and wireless network backup, and its high reliability and convenient networking make it suitable for large-scale distributed industrial applications. Such as smart lockers, charging piles, bank ATM machines, tower monitoring, electricity, water conservancy, environmental protection".

Several vulnerabilities in the H8922 device allow remote attackers to cause the device to execute arbitrary commands with root privileges due to the fact that user provided data is not properly filtered as well as a backdoor account allows access via port 5188/tcp.

CVE

CVE-2021-28149, CVE-2021-28150, CVE-2021-28151, CVE-2021-28152

Credit

An independent security researcher, Konstantin Burov / @_sadshade, has reported this vulnerability to the SSD Secure Disclosure program.

Affected Versions

Hongdian H8922 version 3.0.5

Vendor Response

The vendor has been informed more than 30 days ago about the vulnerabilities, subsequent attempts to email and report the vulnerabilities went unanswered.

Vulnerability Analysis

Hidden Functionality (Backdoor)

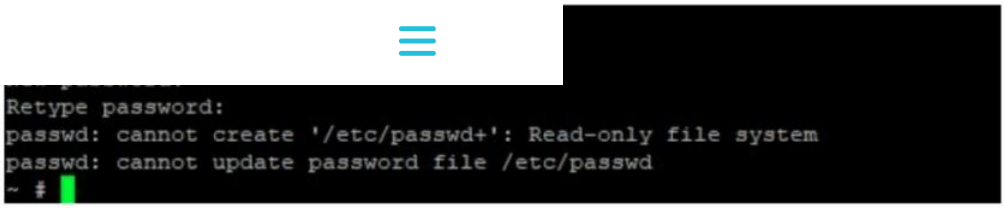
The device has an undocumented feature that allows access to shell as a superuser. To connect, the telnet service is used on port 5188 with the default credentials – *root:superzxmn.*

This method of connection, as well as credentials, are not described in the
documentation for the device and therefore are considered an undocumented possibility for remote control.

Attackers can use this feature to gain uncontrolled access to the device.

Use of Hard-coded Credentials

The root password cannot be changed in the normal way, which prevents unauthorized people from connecting to the device.

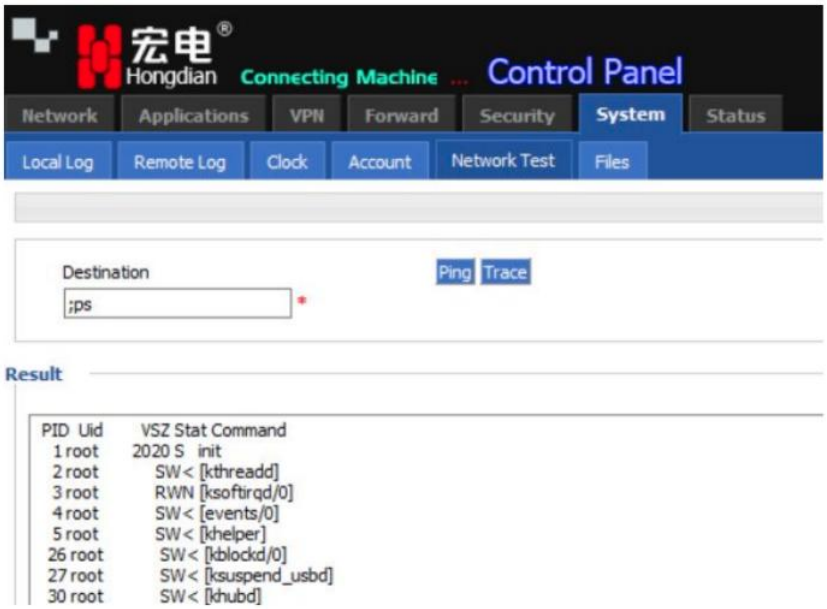


Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

The */tools.cgi* handler, which is responsible for network diagnostics (ping), does not filter user data in the "destination" parameter.

A remote attacker with minimal privileges (guest) can execute an arbitrary command of the operating system as the superuser (root) by substituting the command end character.

For example, the string "*;ps*" entered in the ip-address field displays the list of processes running on the system.

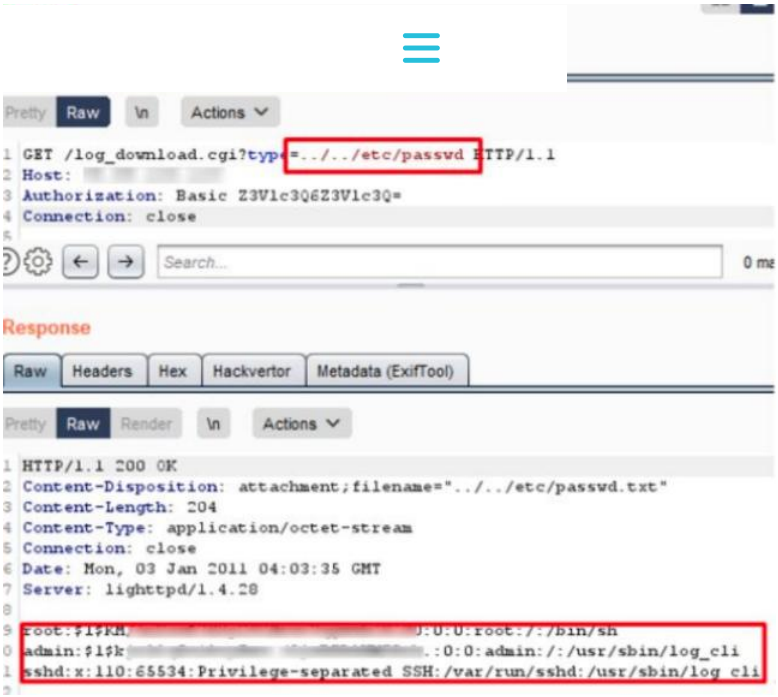


Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

The */log_download.cgi* log export handler does not validate user input and allows a remote attacker with minimal privileges to download any file from the device by substituting "*../*" for example "*../../etc/passwd*".

The check can be carried out using an Internet browser by changing the file name accordingly.

You need to follow the link *http://[ip]/log_download.cgi?type=../../etc/passwd*, log in and the web server will allow download the contents of the "*/etc/passwd*" file.



Insecure direct object references to static files

The unprivileged user “guest” can access the file with the system configuration of the device (cli.conf) via the direct link *http://[ip]/backup2.cgi*.

The file can be used to reveal administrator password and other sensitive data.

```
!
service webadmin
```

Get in touch

Any questions? Interested in our services?
We’d love to hear from you

CONTACT US