“CVE-2024-6387” Statement

Publication date: 2024 December 19

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed vulnerability “CVE-2024-6387”.

Executive Summary

As detailed in the item CVE-2024-6387 published in the NIST National Vulnerability Database (NVD), a security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger the vulnerability by failing to authenticate within a set time period.

NVD indicates an overall CVSS score of 8.1, evaluated by RedHat, Inc. which is considered high. The vector is (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

This vulnerability could concern medical devices which utilize the OpenSSH protocol.

Successful exploitation of this vulnerability may allow a threat actor to perform remote software control on a device or system.

The segments of the Fresenius group are actively monitoring the “CVE-2024-6387” and analysis actions were taken to determine the impact on our current products.

Fresenius products assessment

The following list of products **are affected by CVE-2024-6387**.

Fresenius Kabi

Product	Versions
Infusion Pump - Ivenix LVP SW-0005	5.9.1 and earlier

CVE-2024-6387 impact rationale

General impacts:
Successful exploitation of these vulnerabilities may allow a threat actor to perform remote software control of the Ivenix LVP SW-0005.
Impact to individual organizations depends on many factors that are unique to each organization. Fresenius recommends that organizations apply recommended IT security measures to install and run the product and evaluate the impact of this vulnerability based on their operational environment and specific clinical usage.

The OpenSSH sshd login grace time expiry message is issued from signal handler context where it is not safe and may cause heap corruption, potentially leading to remote code execution.

Risk control measures and compensating controls:
To exploit this vulnerability in the OpenSSH software, an attacker must have direct or adjacent network access and physical access to the single LVP under attack. They must then enable a rarely used Remote Login accessible from the service mode which requires a hospital-defined password. Additionally, the complexity of the attack is considered high, as it requires knowledge of how to enable and access Remote Login and the ability to perform remote code execution.

Service pack (upgrade to 5.9.2), presently available to customers fixes the vulnerability.

Ivenix LVP SW-0004 users shall ensure the products are installed and used as intended according to the products accompanying documentation. Additionally, service pack shall be installed as soon as possible.

Residual Risk Rationale
This exploit is considered complex given the design mitigations present in the LVP-SW system. The service pack effectively fixes the vulnerability.

Ivenix LVP SW-0005 users are strongly encouraged to ensure that the Ivenix Infusion System is installed and maintained as suggested by the Fresenius Kabi Implementation Services team.

Applying LVP-SW 5.9.2 service pack as soon as possible allows to remediate this vulnerability.
Customers should also limit the use of Remote Login within Service Mode and apply best practices for system security.

The following weaknesses are associated with “CVE-2024-6387”:

CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-364	Signal Handler Race Condition

General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate Medical Devices into your IT infrastructure. The Fresenius Group recommends operators of Medical Devices and software to incorporate the following industry best practices into their defense-in-depth strategy:

- Conduct a comprehensive and periodic security risk assessment on the medical network in accordance with operational security best practices such as ISO 27002
- Minimize network exposure for all medical devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius Medical Devices behind firewalls, in dedicated medical networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated medical network
- Implement application firewalls capable of deep packet inspection to help protect against zero-day vulnerabilities and the latest exploits
- Use appropriate authentication and authorization of users on the network
- Implement physical controls that ensure no unauthorized persons would have access to the medical devices and systems
- Ensure that all programming software and equipment (service laptops, etc.) are kept in locked cabinets and are never connected to any network other than the medical network they are intended to service
- Ensure that all portable media used for data exchange with the medical network (such as CDs, USB drives, etc.) are scanned before use
- Implement a process to monitor, prevent and contain malwares and computer viruses.

Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but not limited to: Data Leak, Data Corruption, Data Loss, Network or Service Outage, etc.

References

Regarding “CVE-2024-6387” more details can be found on:

NVD reference: https://nvd.nist.gov/vuln/detail/CVE-2024-6387
MITRE reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6387
CERT-EU security advisory: https://cert.europa.eu/publications/security-advisories/2024-066/

Contacts

For any questions or suggestions please contact your regional marketing manager.