Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Uncontrolled search path element vulnerability in Vyaire Upgrade Utility on Windows XP

Date: 2019- 03-08 **DocumentID: SEC-01-180926**

Background

Vyaire Medical was made aware of an uncontrolled search path element vulnerability (CWE-427) within Upgrade Utility version 2.0.2.2 and prior version on Windows XP. Successful exploitation of this vulnerability may allow an attacker to insert a malicious DLL on the target system and run arbitrary code.

Response

Affected Products

- Vyaire Upgrade Utility versions 2.0.2.2 and prior on Windows XP

The vulnerability can be exploited with local access to a system where the Vyaire Upgrade Utility is installed.

The attack complexity is low as the attacker needs to place a malicious DLL in the Upgrade Utility's program folder, the level of privileges required is high as administrative privileges for write access to the folder are required.

User interaction is not required if the attacker has the privileges to execute the Upgrade Utility, otherwise it is necessary for a user to start the application to trigger the exploit. Scope is unchanged while impacts on confidentiality, integrity and availability are rated high as the attacker may run arbitrary code on the target system under the user's account.

A CVSS v3.0 base score of 6.7 (medium) has been calculated.
The vector string is: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Mitigations & Compensating Controls

Vyaire Medical is no longer supporting the Vyaire Upgrade Utility for use with Windows XP systems.

Vyaire Medical recommends its customers to upgrade to the newer Vyaire Upgrade Utility 2.0.3.0.

This updated Upgrade Utility will not install on Windows XP and will require updating the underlying system to Windows 7 or later.

The newest version of the Vyaire Upgrade Utility, version 2.0.3.0, is available. Please contact your Vyaire field service representative to get a download link for this update.

Generic controls

Vyaire recommends that users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Do not upload and run untrusted files without verifying the integrity of the file.
- Interact with, and only obtain files, software, and software patches from trustworthy highly reputable sources.
- Ensure that employees with access to the Vyaire Upgrade Utility are fully aware of the ongoing potential for social engineering attacks and are trained to identify and avoid social engineering attacks.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

For additional technical details and indicators associated with this vulnerability, review ICSMA-18-037-01 and CVE-2018-5457.

For product or site-specific concerns, contact your Vyaire service representative.

For more information on Vyaire's proactive approach to product security and vulnerability management, contact us under: http://www.vyaire.com/productsecurity

VYR-GBL-1900004