The WebOrion Software Solutions

Remote Code Execution

www.theweborion.com info@theweborion.in

THE WEBORION SOFTWARE SOLUTION

Remote Code Execution or RCE has been one of the most preferred methods by hackers to infiltrate into a network/machines.

Remote code execution is the ability an attacker has to access someone else's computing device and make changes, no matter where the device is geographically located.

In simple words, Remote Code Execution occurs when an attacker exploits a bug in the system and introduces a malware.

The malware will exploit the vulnerability and help the attacker execute codes remotely. This is akin to actually handing over the control of your entire PC to someone else with all admin privileges.

Remote Code Explanation and Example

Code Injection or Remote Code Execution (RCE) enables the attacker to execute malicious code as a result of an injection attack. Code Injection attacks are different than Command Injection attacks.

Attacker capabilities depend on the limits of the server-side interpreter (for example, PHP, Python, and more). In some cases, an attacker may be able to escalate from Code Injection to Command Injection.

The best way to protect a computer from a remote code execution vulnerability is to fix holes that allow an attacker to gain access.

Example of Remote Code Execution

Example:1

An employee browses the Internet with the Internet Explorer browser and visits a website, which they were prompted to visit via an unsuspecting email message. Little do they know that the website exploits a bug on their browser, allowing for remote execution of code to occur.

The code is set up by a criminal who has programmed it to run on the employee’s computer, and in turn, installs a Trojan virus. A Trojan allows a back door into the computer, which can be accessed at any time by the attacker.

At this point, the criminal has complete access to the employee’s data files and will do as they please with it.

Example of Remote Code Execution

Example:2

A business runs an unsupported version of Windows on a computer, which happens to be Windows XP. An employee visits a website, however this website has been compromised, and a bug detects the user working on a computer that has Windows XP.

Since this particular operating system is no longer patched by Microsoft, vulnerabilities are eminent. The bug picks up on this and begins remote code execution, set up by a criminal, to run ransom-ware on your computer.

The ransom involves the criminal holding the company’s files hostage until payment is made.

How can you protect against Remote Code Execution

- The most practical way to approach this is to patch up the vulnerabilities found on all computers over the network, especially those used by administrators. To look at it another way, any available holes are waiting to be exploited which can potentially permit an attacker entry onto the computer system, where they can run any malicious code they want.

- Be sure to upgrade from unsupported operating systems, such as Windows XP, to make sure that your systems aren’t an easy target to attackers.

About TheWeborion

- WebOrion™ – Trusted brand since 2012 for Cyber Security
- Our experts convert ideas into reality and add value to our customers by providing quality Cyber Security solutions.
- We thrive in providing security to all types of applications focusing on preventing cyber attacks and data clean-up after cyber incident.

Learn more:

Phone: +1-(202)-765-7053

Email: info@theweborion.com

Website: www.theweborion.com