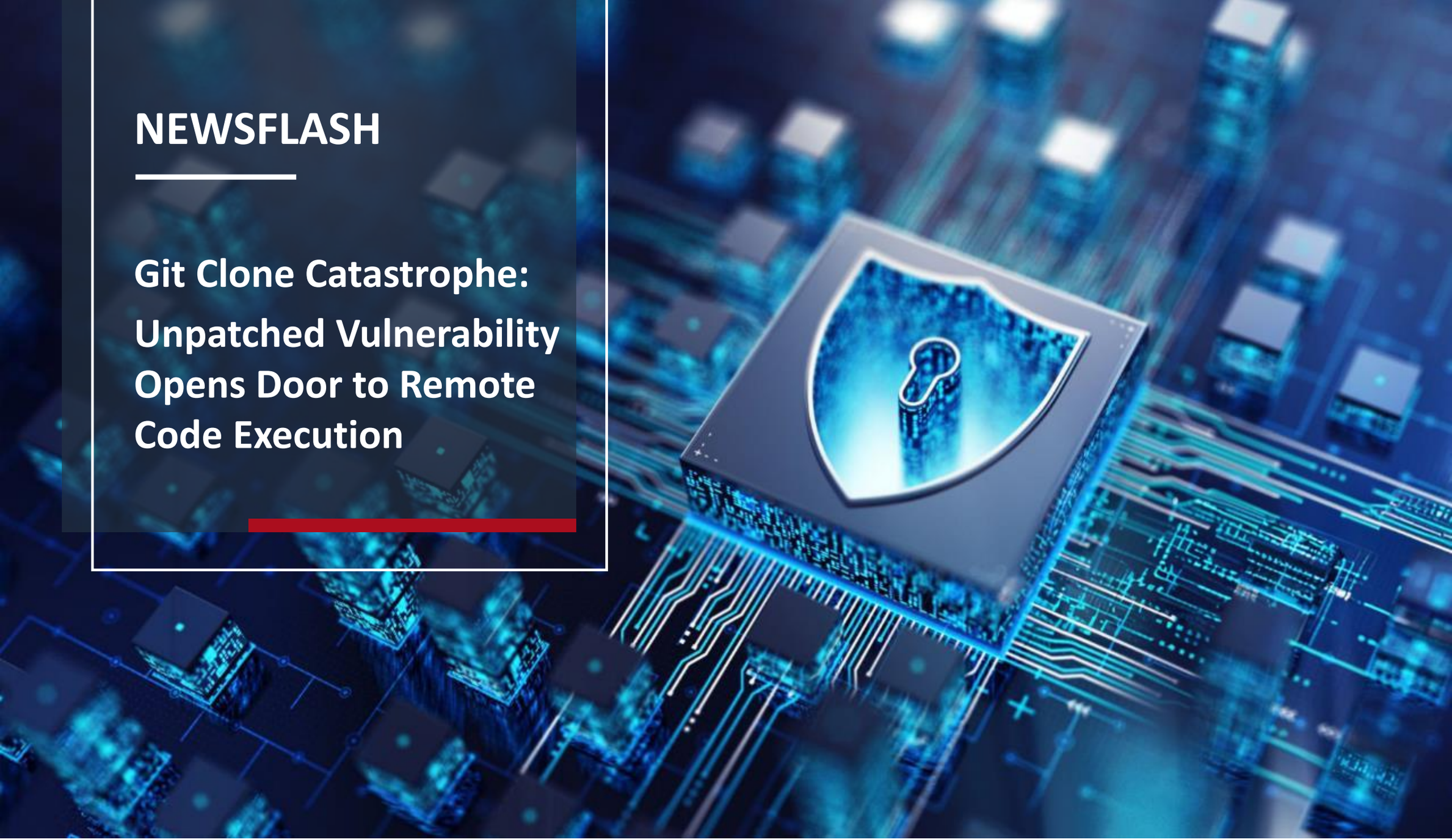


NEWSFLASH

Git Clone Catastrophe: Unpatched Vulnerability Opens Door to Remote Code Execution

NANGIA & CO LLP

What is the RCE Vulnerability while Cloning Git Repositories?

A critical Remote Code Execution (RCE) vulnerability has been identified in the process of cloning Git repositories. This issue arises when repositories containing submodules are manipulated to exploit a flaw in Git, allowing files to be written not in the submodule's work tree but directly into the ".git/" directory. This exploit causes a hook to execute during the cloning process, giving users no opportunity to inspect or interrupt the code execution. As a result, this vulnerability poses a significant security risk, as it enables automatic code execution without user verification. Malicious actors can leverage repositories with submodules to exploit this bug, leading to the execution of a hook from the ".git/" directory during the cloning process, and potentially resulting in Remote Code Execution (RCE). This type of attack is especially dangerous because it can provide attackers with control over the system, allowing them to run arbitrary code, install malware, or carry out other malicious actions without the user's knowledge or consent. The RCE vulnerability while cloning Git repositories underscores the critical security concern identified as CVE-2024-32002.

What is affected?

Version prior to 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4 are affected.

How to check if you are running a vulnerable version?

Here are a few steps to follow check the running version of Git in system.

Step 1

Launch your terminal (Linux, macOS), command prompt (Windows), or any preferred command-line interface

Step 2

Type **git --version** and hit Enter to run the command.

What is the risk?

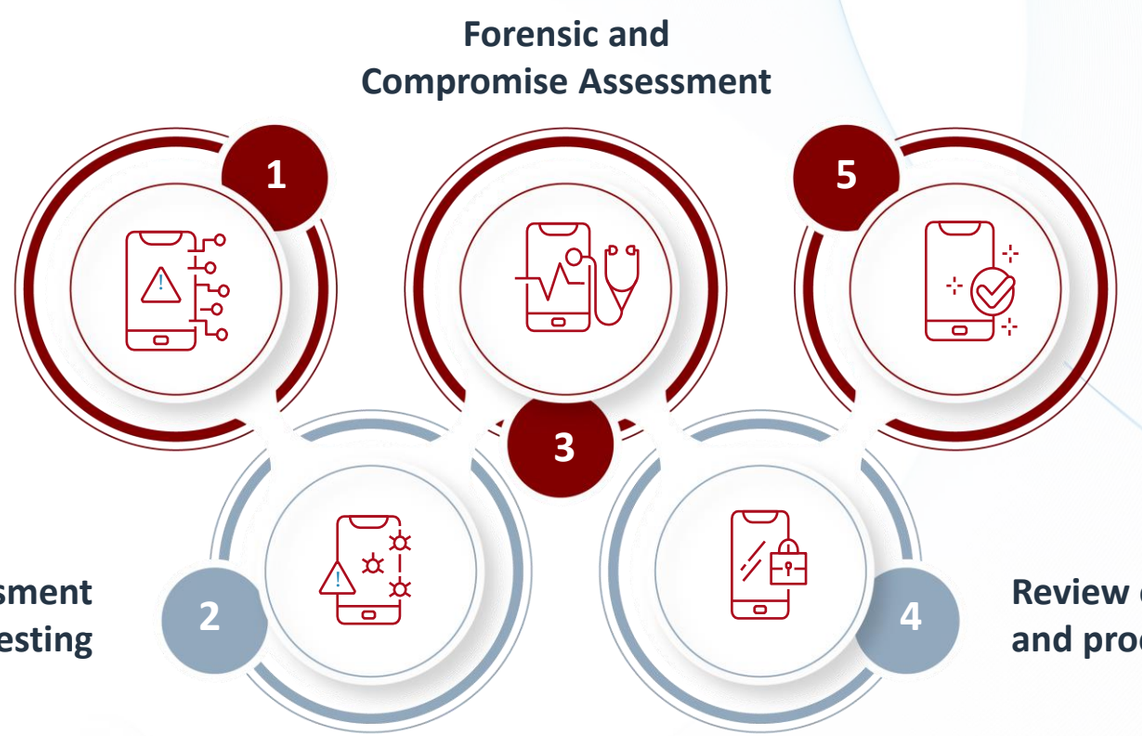
This vulnerability enables attackers to remotely execute arbitrary code on the compromised system, potentially granting them full control to run any commands or programs they wish. The exploit is automatically triggered during the cloning of a Git repository, without any user intervention. This automatic execution heightens the risk, as users are unaware and unable to prevent the attack during the cloning process. Once the vulnerability is exploited, attackers can perform various malicious activities such as installing malware, exfiltrating data, or incorporating the system into a botnet. Developers who clone repositories from platforms like GitHub, GitLab, or others are particularly at risk. The extensive use of Git in development environments amplifies the potential impact. Given Git's widespread popularity, this vulnerability can affect a vast number of systems, making it a prime target for attackers.

How do you protect yourself?

Some of the steps that can be undertaken to protect the organization's infrastructure are:

1. It is important to upgrade the Git to latest versions(Git v2.45.1, v2.44.1, v2.43.4, v2.42.2, v2.41.1, v2.40.2, and v2.39.4.) is essential to protect from such critical vulnerability.
2. Also recommended to disable Symbolic link support (via git config --global core.symlinks false). It eliminates possibility of such attacks.
3. Clone and inspect repositories within a containerized or sandboxed environment to limit the potential impact of any malicious code. Tools like Docker can be used to create isolated environments.
4. Ensure that the user account performing Git operations has the minimum necessary permissions. Avoid using accounts with administrative or root privileges for cloning repositories.
5. Conduct regular Vulnerability Assessment and Penetration tests for all public and internal facing information systems in your organization.
6. Conduct Comprise Assessments to proactively check for any signs of compromise of your IT environment.

How can Nangia & Co LLP help?



NOIDA
(Delhi NCR - Corporate Office) A-109, Sector - 136, Noida - 201304, India
T: +91 120 2598000

DELHI
(Registered Office) B-27, Soami Nagar, New Delhi - 110017, India T: +91 120 2598000

GURUGRAM
001-005, Emaar Digital Greens Tower-A 10th Floor, Golf Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

MUMBAI
4th Floor, Iconic Tower, URMI Estate, Ganpat Rao Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

CHENNAI
Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand Lights, Chennai - 600006 T: +91 44 46549201

BENGALURU
Prestige Obelisk, Level 4, No 3 Kasturba Road, Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

PUNE
3rd Floor, Park Plaza, CTS 1085, Ganeshkhind Road, Next to Pune Central Mall, Shivajinagar, Pune - 411005, India

DEHRADUN
1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001, Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

Follow us at: