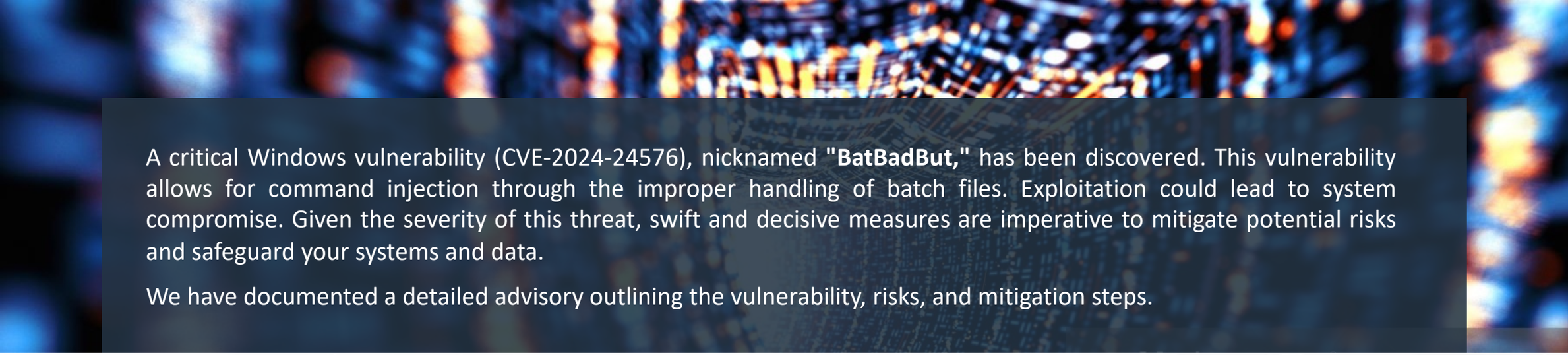
NEWSFLASH

“BatBadBut” Bug Bites: Critical Windows Injection Flaw

NANGIA & CO LLP



A critical Windows vulnerability (CVE-2024-24576), nicknamed **"BatBadBut,"** has been discovered. This vulnerability allows for command injection through the improper handling of batch files. Exploitation could lead to system compromise. Given the severity of this threat, swift and decisive measures are imperative to mitigate potential risks and safeguard your systems and data.

We have documented a detailed advisory outlining the vulnerability, risks, and mitigation steps.

What is “BatBadBut” Vulnerability

The BatBadBut Vulnerability is a critical flaw affecting the handling of batch files (bat and cmd extensions) on Windows platforms across various programming languages/ technologies. It allows attackers to execute arbitrary shell commands by bypassing the escaping mechanism. This vulnerability may also affect the application that executes commands without specifying the file extension.

Background of Vulnerability

Flatt Security has discovered a critical vulnerability called BatBadBut "bad, but not the worst" that could allow attackers to inject malicious commands into Windows applications. The flaw, discovered by Flatt Security’s security engineer RyotaK, affects multiple programming languages. It was reported to the CERT Coordination Center and registered as CVE-2024-24576 on GitHub with a severity score of 10.0.

Who is affected?

The vulnerability affects multiple programming languages on Windows platforms. Specifically, developers who invoke batch files with untrusted arguments are at risk. Below is the table of the status of the affected Programming languages with their respective CVEs:

Language	Affected Version	CVE
Haskell Programming Language	1.0.0.0, 1.0.1.1, 1.0.1.2, 1.0.1.3, 1.0.1.4, 1.0.1.5, 1.1.0.0, 1.1.0.1, 1.1.0.2, 1.2.0.0, 1.2.1.0, 1.2.2.0, 1.2.3.0, 1.3.0.0, 1.4.0.0, 1.4.1.0, 1.4.2.0, 1.4.3.0, 1.5.0.0, 1.6.0.0, 1.6.1.0, 1.6.2.0, 1.6.3.0, 1.6.4.0, 1.6.5.0, 1.6.5.1, 1.6.6.0, 1.6.7.0, 1.6.8.0, 1.6.8.1, 1.6.8.2, 1.6.9.0, 1.6.10.0, 1.6.11.0, 1.6.12.0, 1.6.13.0, 1.6.13.1, 1.6.13.2, 1.6.14.0, 1.6.15.0, 1.6.16.0, 1.6.17.0, 1.6.18.0	CVE-2024-3566
Rust	All Rust versions before 1.77.2 on Windows are affected	CVE-2024-24576, CVE-2024-3566
yt-dlp	>=2021.04.11, <2024.04.09	CVE-2024-3566, CVE-2024-22423
Node.js	Versions up to, including, (<=) 21.7.2	CVE-2024-3566

Note: There may be other programming languages which may be affected. It is advised to check with the with the individual entities which manage the pertinent programming languages used.

What is the risk?

Attackers may exploit this vulnerability to run arbitrary shell commands, possibly resulting in unauthorized access, data breaches, and or system compromise.

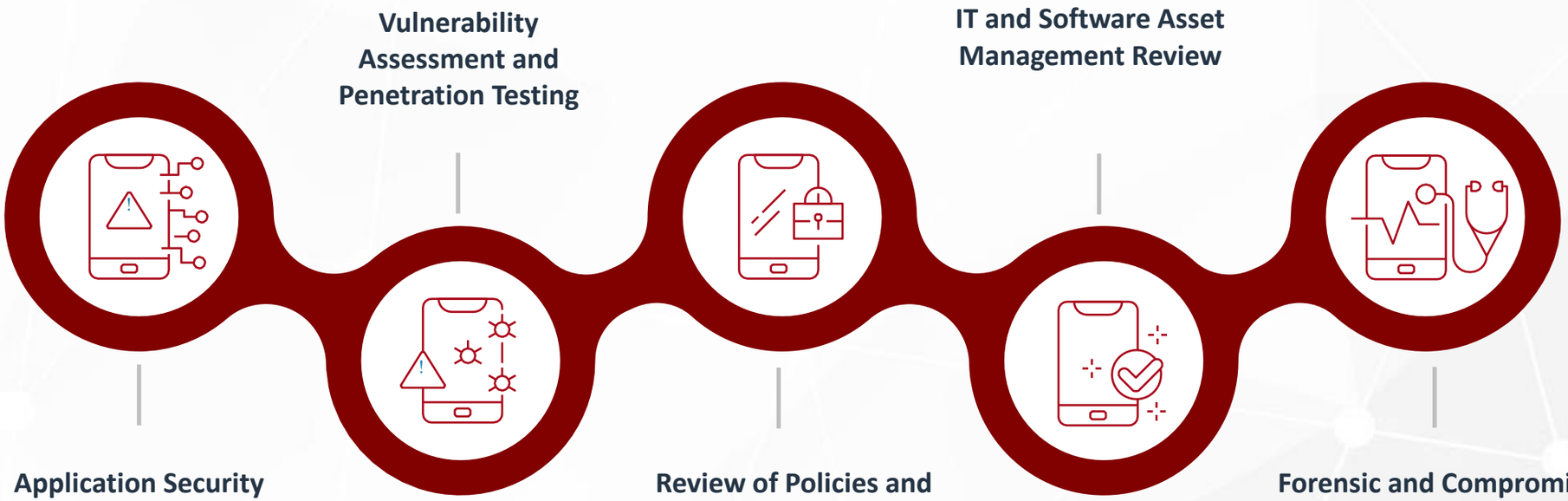
Note: The impact of this vulnerability varies from application to application and is subject to the implementation of the module handling batch files in the vulnerable programming language.

How do you protect yourself?

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

1. Update the relevant patches as per the vendor releases.
2. Develop proper escaping rules for command arguments to prevent potential command injection attacks. Additionally, move batch files to directories outside the PATH environment variable to reduce the risk of unexpected execution.
3. Regularly assess your systems and applications for vulnerabilities. This can include penetration testing, vulnerability scanning, and code review to identify and address potential security weaknesses.

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:

NANGIA & CO LLP