UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0269

GIT PATCHES TWO RCE SECURITY FLAWS

DATE ISSUED: 23rd January 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Git has patched two severe security vulnerabilities that could allow attackers to exploit heap-based buffer overflow weaknesses in the Git's code to execute malware.

BREAKDOWN

Git has a range of products based around a Version Control System (VCS) that allows users to collaborate on code by keeping track of code changes. Security experts from X41 D-SEC GmbH and GitLab found a total of eight vulnerabilities in Git's code out of which two critical vulnerabilities are tracked as CVE-2022-41903 and CVE-2022-23521. They allow an attacker to exploit integer buffer overflow in a system's memory which may result into Remote Code Execution (RCE). A buffer overflow happens when a program is trying to input a huge value or number that is greater than an integer type can store. A patch has been released for the two critical vulnerabilities. A third Windows specific flaw that impacts the Git GUI tools which allows an attacker to run untrusted code attacks by exploiting an untrusted search path weakness does not have a patch available, but users can mitigate its effects by avoiding the use of the Git GUI software to clone repositories or avoid cloning from an untrusted source.

REMEDIATION STEPS

- Upgrading to the latest version of Git.
- Update all GitLab instances.
- Disabling the 'git archive' in untrusted repositories.

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/git-patches-two-critical-remote-code-execution-security-flaws/

Malwarebytes https://www.malwarebytes.com/blog/news/2023/01/update-now-two-critical-flaws-in-gits-code-found-patched