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

CYBER GUIDANCE ISSUE 00102

DEPENDENCY CONFUSION ATTACKS

DATE ISSUED: 15th February 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A number of high-stakes companies have paid bug bounties to a group of ethical hackers after the discovery of flaws in their software development based on dependency confusion attacks utilizing public and private library repository packages.

BREAKDOWN

Dependency confusion attacks, also known as substitution attacks, occur when an attacker uploads code impersonating existing packages or by using unused names for packages. This enables attackers to hide malicious code inside private code repositories by registering internal library names on public package indexes. Taking advantage of package managers which download and import libraries used during software development, an attacker may be able to exfiltrate highly sensitive information, execute code remotely, or install a backdoor to gain access to a system or network. This type of attack has been tested in a number of repositories just as npm, RubtGems, PyPI, JFrog and NuGet and resulted in the compromised of 35 major technology companies including PayPal, Yelp, Microsoft, Apple, Shopify, Netflix and Uber. Most of the companies listed where the vulnerability has been identified have implemented fixes.

REMEDIATION STEPS

- Do not publish sensitive files (such as package.json) in public locations (e.g. web or source code repositories) and make sure all publicly published content has had appropriate steps taken to minimise the information and reduce exposed attack surface.
- Consider using fully qualified sources for internal packages - either URL's, Git repositories, or Local filesystem sources.
- Ensure that build environments have endpoint protection in case malicious code slips in .
- Use automated/unit testing to validate that resulting builds are functional.

REFERENCES & RESOURCES

Alex Birsan https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
ZDNet: https://www.zdnet.com/article/microsoft-warns-enterprises-of-new-dependency-confusion-attack-technique/