info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00127

NETMASK NETWORKING BUG AFFECTS THOUSANDS

DATE ISSUED: 29th March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Hundreds of thousands of applications are potentially impacted by a critical networking vulnerability discovered in the popular npm library – netmask.

BREAKDOWN

Netmask is used by masses of applications, 3 million downloads per week, to parse and compare IPv4 and CIDR blocks which can be addled by an IP address with a leading zero. Improper validations causes netmask to read a different IP address, translating a decimal formal IP address into an octal format. In most cases, this is stripped and ignore by netmask, however, should an attacker specially craft an IP address, they may be able to conduct a Server-Side Request Forgery (SSRF) and force a connection to a different IP address. There is also the potential that this flaw may be exploited for Remote File Inclusion (RFI) to force a server to reference external scripts in order to upload malware. Creative attackers may find all sorts of ways to exploit this vulnerability that is being tracked as CVE-2021-28918.

REMEDIATION STEPS

- Install the latest version of npm netmask, version 2.0.0 that includes fixes. Resource included below.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/
NPM	https://www.npmjs.com/package/netmask