UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 0011

CRITICAL SAP NETWEAVER JAVA FLAW

DATE ISSUED: 14th July 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	LOW	MEDIUM	[✓ HIGH]

OVERVIEW

Successful exploitation of the Remote Execution of Code On NetWeaver (RECON) bug (CVE-2020-6287) opens a back door to full system administration giving the ability to read, write, modify and execute a range of files, functions and activities.

BREAKDOWN

Given that SAP is a prominent Enterprise Resource Planning (ERP) software for managing human resources, finances, logistics and customer facing faces, the system contains multitudes of sensitive data. Attackers would be able to read and modify financial records, have access to Personal Identifiable Information (PII), create and complete purchases, execute code, modify and delete logs, traces and any other files, as well as general sabotage of operations or operating system command and control. The vulnerability exists in SAP NetWeaver Java v7.3-7.5 which is a default component of every SAP and is presented through a lack of authentication in one of the web components, whereby a remote attacker may create administrative accounts with elevated privileges. Due to the interconnected nature of the SAP system to other systems in a trust relationship, it would be simple enough for an attacker or malware to move laterally across a network. Thus far there are no recorded attacks, though following the announcement the risk of attack will have increased.

REMEDIATION STEPS

- Download and install security patch incorporated as part of SAP July 2020 Security Note

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/critical-sap-bug-enterprise-system-takeover/157392/
ZDNet	https://www.zdnet.com/article/recon-bug-lets-hackers-create-admin-accounts-on-sap-servers/
Security Affairs	https://securityaffairs.co/wordpress/105861/hacking/sap-recon-flaw.html