U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00133

SAP BUGS UNDER ACTIVE ATTACK

DATE ISSUED: 12th April 2021

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

OVERVIEW

A range of attacks have been carried out on vulnerable SAP mission critical systems, causing widespread compromise, theft of sensitive data and disruption to organisations.

BREAKDOWN

Data theft, financial fraud, disruption to services and other operations, delivery of malware and ransomware have all been seen in a recent onslaught of at least 300 attacks focussing on SAP applications used to manage processes, product lifecycles, customer relationships and supply chains. High-privilege users are suffering brute force attacks as well as the following known bugs being under active exploitation: CVE-2020-6287, CVE-2020-6207, CVE-2018-2380, CVE-2016-9563, CVE-2016-3976 and CVE-2010-5326. The breadth of the attacking groups, attacks themselves, and techniques used to conduct them is wide-ranging, with some being "weaponised in less than 72 hours" after patches were released.

REMEDIATION STEPS

- Apply all available patches to SAP applications where they are available.
- Use unique passwords for all accounts that are web-facing.
- Enable 2FA where possible.
- Isolate devices with vulnerable SAP applications from the main corporate network until patches can be applied.
- Use monitoring and protective devices and software to detect and respond to indications of compromise in a timely manner.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/sap-bugs-cyberattack-compromise/165265/
US CERT	https://us-cert.cisa.gov/ncas/current-activity/2021/04/06/malicious-cyber-activity-targeting-critical-sap-applications
ZDNet	https://www.zdnet.com/article/sap-issues-advisory-on-vulnerable-applications-being-widely-targeted-by-hackers