NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÉ VAROVANIE

No: V20200610-04K

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Kritické zraniteľnosti v SAP produktoch

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie kritické bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2018-1000632, CVE-2019-0319, CVE-2019-17571, CVE-2020-1938, CVE-2020-6239, CVE-2020-6246, CVE-2020-6260, CVE-2020-6263, CVE-2020-6264, CVE-2020-6265, CVE-2020-6266, CVE-2020-6268, CVE-2020-6269, CVE-2020-6270, CVE-2020-6271, CVE-2020-6275, CVE-2020-6279

Zasiahnuté systémy

SAP Liquidity Management for Banking verzia 6.2
SAP Commerce verzia 6.7, 1808, 1811, 1905
SAP Commerce (Data Hub) verzie 6.7, 1808, 1811, 1905
SAP SuccessFactors Recruiting verzie 2005
SAP Solution Manager (Problem Context Manager) verzia 7.2
SAP Netweaver AS ABAP verzie 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754
SAP NetWeaver AS JAVA (P4 Protocol)
SAP-JEECOR 7.00, 7.01; SERVERCOR 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; CORE-TOOLS 7.00, 7.01, 7.02, 7.05, 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
SAP Fiori for SAP S/4HANA verzie 200, 300, 400, 500
SAP ERP (Statutory Reporting for Insurance Companies);
Versions - EA-FINSERV 600, 603, 604, 605, 606, 616, 617, 618, 800; S4CORE 101, 102, 103, 104
SAP Business One (Backup service) verzie 9.3, 10.0
SAP Gateway verzie 7.5, 7.51, 7.52 and 7.53
SAP Business Objects Business Intelligence Platform verzia 4.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava
Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915
SK-CERT
Naša značka:
01439/2020/SK-CERT-142

BEZPEČNOSTNÉ VAROVANIE

Zdroje
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=547426775

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01439/2020/SK-CERT-142