NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÉ VAROVANIE

No: V20200610-05K

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

Identifikátor

Intel produkty viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti sa nachádzajú v Intel® Active Management Technology (AMT) konfigurovaných pre IPv6 a umožňujú vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2020-0531, CVE-2020-0532, CVE-2020-0533, CVE-2020-0534, CVE-2020-0535, CVE-2020-0536, CVE-2020-0537, CVE-2020-0538, CVE-2020-0539, CVE-2020-0540, CVE-2020-0541, CVE-2020-0542, CVE-2020-0545, CVE-2020-0566, CVE-2020-0586, CVE-2020-0594, CVE-2020-0595, CVE-2020-0596, CVE-2020-0597, CVE-2020-8674

Zasiahnuté systémy

Intel® CSME, Intel® AMT, Intel® ISM, Intel® DAL and Intel® DAL verzie staršie ako 11.8.77, 11.12.77, 11.22.77, 12.0.64, 13.0.32, 14.0.33, 14.5.12
Intel® Server Platform Services verzie staršie ako SPS_E5_04.01.04.380.0, SPS_SoC-X_04.00.04.128.0, SPS_SoC-A_04.00.04.211.0, SPS_E3_04.01.04.109.0, SPS_E3_04.08.04.070.0

Následky

Eskalácia privilégií
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html

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-143