



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Zoom viacero zraniteľností

Popis

Spoločnosť Zoom vydala bezpečnostnú aktualizáciu na svoj produkt Zoom, ktorá opravuje viacero bezpečnostných zraniteľností.

Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.06.2020

CVE

CVE-2020-6109, CVE-2020-6110

Zasiahnuté systémy

Zoom verzie staršie ako 4.6.12

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame 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.

Zdroje

https://talosintelligence.com/vulnerability_reports/TALOS-2020-1056

https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055

<https://thehackernews.com/2020/06/zoom-video-software->

[hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29](https://thehackernews.com/2020/06/zoom-video-software-hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29)