Los grupos de estado-nación iraníes ahora se unieron a hackers motivados financieramente para explotar una vulnerabilidad crítica en el software de gestión de impresión PaperCut, según revelaciones Microsoft del fin de semana.

El equipo de inteligencia de amenazas de la compañía dijo que observó que Mango Sandstorm (Mercury) y Mint Sandstorm (Phosphorus) armaron CVE-2023-27350 en sus operaciones para lograr el acceso inicial.

> *«Esta actividad muestra la capacidad continua de Mint Sandstorm para incorporar rápidamente exploits en sus operaciones»,* dijo Microsoft.

Por otro lado, se dice que la actividad de explotación de CVE-2023-27350 asociada con Mango Sandstorm está en el extremo inferior del espectro, con el grupo patrocinado por el estado *«usando herramientas de intrusiones anteriores para conectarse a su infraestructura C2».*

Cabe mencionar que Mango Sandstorm está vinculado al Ministerio de Inteligencia y Seguridad de Irán (MOIS) y Mint Sandstorm está asociado con el Cuerpo de la Guardia Revolucionaria Islámica (IRGC).

El ataque en curso se produce semanas después de que Microsoft confirmara la participación de Lace Tempest, un grupo hackers que superpone a otros grupos como FIN11, TA505 y Evil Corp, en el abuso de la vulnerabilidad para entregar el ransomware Cl0p y LockBit.

CVE-2023-27350 (puntaje CVSS: 9.8) se relaciona con una vulnerabilidad crítica en las instalaciones de PaperCut MF y NG que podría ser aprovechada por un atacante no autenticado para ejecutar código arbitrario con privilegios de SYSTEM.

PaperCut puso a disposición un parche del 8 de marzo de 2023. Se espera que Zero Day Initiative (ZDI) de Trend Micro, que descubrió e informó el problema, publique más

información técnica al respecto el 10 de mayo de 2023.

Además, la compañía de seguridad cibernética VulnCheck, la semana pasada, publicó detalles sobre una nueva línea de ataque que puede eludir las detecciones existentes, permitiendo así a los hackers aprovechar la vulnerabilidad sin obstáculos.

Con más atacantes explotando PaperCut para violar servidores vulnerables, es imperativo que las organizaciones se muevan rápidamente para aplicar las actualizaciones necesarias (versiones 20.1.7, 21.2.11 y 22.0.9 y posteriores).

El desarrollo también sigue a un informe de Microsoft que reveló que los hackers iraníes confían cada vez más en una nueva táctica que combina operaciones cibernéticas ofensivas con operaciones de influencia en múltiples frentes para *«impulsar el cambio geopolítico en consonancia con los objetivos del régimen»*.

El cambio coincide con un mayor ritmo en la adopción de vulnerabilidades recientemente informadas, el uso de sitios web comprometidos para comando y control para ocultar mejor la fuente de los ataques y el aprovechamiento de herramientas y oficios personalizados para lograr el máximo impacto.