Fortinet ha implementado actualizaciones para solucionar una vulnerabilidad crítica de seguridad que afecta a su solución de control de acceso a la red FortiNAC y que podría resultar en la ejecución de código arbitrario.

Identificado como CVE-2023-33299, el defecto tiene una calificación de severidad de 9.6 sobre 10 en el sistema de puntuación CVSS. Se ha descrito como un caso de deserialización no confiable de objetos en Java.

> *«Una vulnerabilidad de deserialización de datos no confiables [CWE-502] en FortiNAC puede permitir que un usuario no autenticado ejecute código o comandos no autorizados mediante solicitudes especialmente diseñadas al servicio tcp/1050″,* señaló Fortinet en un aviso publicado la semana pasada.

La falla afecta a los siguientes productos, y se han publicado parches en las versiones de FortiNAC 7.2.2, 9.1.10, 9.2.8 y 9.4.3 o posteriores:

- FortiNAC versión 9.4.0 a 9.4.2
- FortiNAC versión 9.2.0 a 9.2.7
- FortiNAC versión 9.1.0 a 9.1.9
- FortiNAC versión 7.2.0 a 7.2.1
- FortiNAC 8.8 todas las versiones
- FortiNAC 8.7 todas las versiones
- FortiNAC 8.6 todas las versiones
- FortiNAC 8.5 todas las versiones
- FortiNAC 8.3 todas las versiones

Fortinet también ha solucionado una vulnerabilidad de severidad media identificada como CVE-2023-33300 (puntuación CVSS: 4.8), un problema de control de acceso inapropiado que afecta a FortiNAC 9.4.0 a 9.4.3 y FortiNAC 7.2.0 a 7.2.1. Se ha corregido en las versiones 7.2.2 y 9.4.4 de FortiNAC.

Florian Hauser, de la firma alemana de ciberseguridad CODE WHITE, ha sido reconocido por descubrir e informar sobre los dos errores.

Esta alerta sigue a la explotación activa de otra vulnerabilidad crítica que afecta a FortiOS y FortiProxy (CVE-2023-27997, puntuación CVSS: 9.2) y que podría permitir que un atacante remoto ejecute código o comandos arbitrarios mediante solicitudes especialmente diseñadas.

Fortinet, a principios de este mes, reconoció que el problema podría haber sido utilizado en ataques limitados dirigidos a sectores gubernamentales, de fabricación e infraestructuras críticas, lo cual llevó a la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) a agregarlo al catálogo de Vulnerabilidades Explotadas Conocidas (KEV, por sus siglas en inglés).

También sucede más de cuatro meses después de que Fortinet solucionara una grave falla en FortiNAC (CVE-2022-39952, puntuación CVSS: 9.8) que podría resultar en la ejecución arbitraria de código. Desde entonces, la vulnerabilidad ha sido objeto de explotación activa poco después de que se haya puesto a disposición un prueba de concepto (PoC).

En un desarrollo relacionado, Grafana ha lanzado parches para una vulnerabilidad crítica de seguridad (CVE-2023-3128) que podría permitir a atacantes maliciosos evadir la autenticación y hacerse cargo de cualquier cuenta que utilice Azure Active Directory para autenticación.

> *«Si se aprovecha, el atacante puede obtener el control total de la cuenta de un usuario, incluido el acceso a datos privados de clientes e información confidencial. Si se aprovecha, el atacante puede obtener el control total de la cuenta de un usuario, incluido el acceso a datos privados de clientes e información confidencial»,* declaró Grafana.