Intel advirtió sobre una vulnerabilidad crítica en el motor de seguridad CSME, por lo que pidió a los usuarios aplicar una solución ya disponible, lo más pronto posible.

El motor de gestión y seguridad convergente de Intel (CSME) es un subsistema de chipset que impulsa las tecnologías de gestión activa de Intel.

Según un aviso de seguridad publicado el martes, CSME está sujeto a una vulnerabilidad de firmware, encontrada internamente por el equipo de seguridad de Intel, que si se explota, permite a los actores de amenazas locales lanzar escalada de privilegios, denegación de servicio y ataques de divulgación de información.

Rastreada como CVE-2019-14598, se le otorgó a la vulnerabilidad una puntuación base de CVSS de 8.2, lo que significa que el problema es crítico.

Intel lanzó una actualización de firmware para mitigar la vulnerabilidad, que afecta las versiones de CSME anteriores a 12.0.49, IOT 12.0.56, 13.0.21 y 14.0.11.

> *«Intel recomienda actualizar a las versiones CSME 12.0.49, 13.0.21 y 14.0.11 o posterior proporcionadas por el fabricante del sistema que aborda estos problemas. Se recomienda a los clientes de IOT que utilicen la versión 12.0.55 de CSME para actualizar a 12.0.56 o posterior proporcionada por el fabricante del sistema que aborda estos problemas»*, dice la compañía.

Otro lote de actualizaciones se dirige a los problemas de seguridad en la RAID Wweb Console 2 (RWC2) de Intel y la RAID Web Console 3 (RWC3 para Windows.

La primera vulnerabilidad, CVE-2020-0562, afecta a todas las versiones de RWC2 y se le otorgó una puntuación base de 6.7, clasificando el error como de gravedad media. Los usuarios locales autenticados pueden aprovechar la falla para escalar sus privilegios, sin embargo, Intel no solucionará el problema.

En cambio, Intel asegura que el producto se descontinuará y recomienda que los usuarios actualicen a RWC3.

El segundo problema de seguridad es el mismo con las mismas consecuencias potenciales. Rastreado como CVE-2020-0564, la falla de seguridad afecta a RWC3 antes de la versión 7.010.009.000.

Manycore Platform Software Stack (MPSS) de Intel, antes de la versión 3.8.6, también recibió una solución para resolver la vulnerabilidad CVE-2020-0563, un problema de gravedad media con un puntaje base de 6.7. La vulnerabilidad puede ser explotada por usuarios no autenticados para permitir la escalada de privilegios por medio del acceso local debido al manejo incorrecto de los permisos.

Intel también mencionó un problema de seguridad de gravedad media, CVE-2020-0560, pero la compañía tampoco emitirá un parche para este problema. El error afecta al controlador Intel Renesas Electronics USB 3.0 y permite la escalada de privilegios en todas las versiones.

> *«Se recomienda que los usuarios del controlador USB 3.0 Intel Renesas Electronics lo desinstalen o suspendan su uso lo antes posible»*, dice Intel.

La compañía también resolvió una vulnerabilidad de baja gravedad en Intel Software Guard Extensions (SGX). Rastreado como CVE-2020-0561, el problema de inicialización incorrecta emitió un puntaje base de 2.5, que puede permitir a los usuarios autenticados escalar sus privilegios por medio del acceso local.