Un investigador de seguridad cibernética reveló ayer públicamente los detalles técnicos y PoC para 4 vulnerabilidades 0-Day sin parches, que afectan a un software de seguridad empresarial ofrecido por IBM luego de que la compañía se negó a reconocer la divulgación presentada responsablemente.

El producto premium afectado en cuestión es IBM Data Risk Manager (IDRM), que ha sido diseñado para analizar los activos de información empresarial confidencial de una organización y determinar los riesgos asociados.

Según Pedro Ribeiro, de la compañía Agile Information Security, IBM Data Risk Manager contiene tres vulnerabilidades de gravedad crítica y una de alto impacto, que se enumeran más adelante, y pueden ser explotadas por un atacante no autenticado accesible por medio de la red, y cuando se encadenan juntos también podrían conducir a la ejecución remota de código como raíz.

- Bypass de autenticación
- Inyección de comandos
- Contraseña predeterminada insegura
- Descarga de archivos arbitrarios

Ribeiro probó con éxito las fallas contra IBM Data Risk Manager versión 2.0.1 a 2.0.3, que no es la última versión del software, pero cree que también funcionan por medio de 2.0.4 a la última versión 2.0.6 porque *«no hay mención de vulnerabilidades fijas en cualquier registro de cambios».*

> *«IDRM es un producto de seguridad empresarial que maneja información muy confidencial. Un compromiso de dicho producto podría conducir a un compromiso de la compañía a gran escala, ya que la herramienta tiene credenciales para acceder a otras herramientas de seguridad, sin mencionar que contiene información sobre vulnerabilidades críticas que afectan a la empresa»*, dijo Ribeiro.

Resumidamente, la falla de omisión de autenticación explota un error lógico en la función de ID de sesión para restablecer la contraseña de cualquier cuenta existente, incluido el administrador.

La falla de inyección de comandos reside en la forma en que el software de seguridad empresarial de IBM permite a los usuarios realizar escaneos de red utilizando scripts Nmap, que aparentemente pueden estar equipados con comandos maliciosos cuando son suministrados por atacantes.

Según la divulgación de vulnerabilidad, para SSH y la ejecución de comandos sudo, el dispositivo virtual IDRM también tiene un usuario administrativo incorporado con nombre de usuario *«a3user»* y contraseña predeterminada *«idrm»,* que de no ser modificada, podría permitir a los atacantes remotos tomar el control total sobre los sistemas específicos.

La última vulnerabilidad reside en un punto final API que permite a los usuarios autenticados descargar archivos de registro del sistema. Sin embargo, según el investigador, uno de los parámetros para este punto final sufre una falla transversal del directorio que podría permitir a los usuarios maliciosos descargar cualquier archivo del sistema.

Además de los detalles técnicos, el investigador también ha lanzado dos módulos Metasploit para omisión de autenticación, ejecución remota de código y problemas de descarga de archivos arbitrarios.

Ribeiro asegura que informó el problema a IBM por medio de CERT/CC y, como respuesta, la compañía se negó a aceptar el informe de vulnerabilidad y dijo: *«Hemos evaluado este informe y cerramos por estar fuera del alcance de nuestro programa de divulgación de vulnerabilidad ya que este producto es solo para soporte 'mejorado' pagado por nuestros clientes».*

En respuesta, Ribeiro dijo que *«En cualquier caso, no solicité ni esperé una recompensa ya que no tengo una cuenta de HackerOne y no estoy de acuerdo con los términos de divulgación de HackerOne o IBM allí. Simplemente quería divulgarlos a IBM de forma*

responsable y dejar que lo arreglen».

Un portavoz informó a The Hacker News que *«un error de proceso dio como resultado una respuesta incorrecta al investigador que informó la situación a IBM. Hemos estado trabajando en los pasos de mitigación y serán discutidos en un aviso de seguridad».*