



Imperva, una de las nuevas compañías de ciberseguridad líderes que ayuda a las empresas a proteger los datos y aplicaciones críticas de los ataques cibernéticos, ha sufrido una violación de datos que expuso información confidencial para algunos de sus clientes, según reveló hoy la compañía.

Esta violación de seguridad afecta de forma particular a los clientes del Firewall de Aplicaciones Web en la Nube (WAF) de Imperva, anteriormente conocido como Incapsula, un servicio CDN centrado en la seguridad conocido por su mitigación DDoS y características de seguridad de aplicaciones web que protegen los sitios web de actividades maliciosas.

En una publicación de hoy, el CEO de Imperva, Chris Hylan, reveló que la compañía se enteró del incidente el 20 de agosto de 2019, solo después de que alguien le informó acerca de la exposición de datos que *«afecta a un subconjunto de clientes de su producto Cloud WAF que tenía cuentas alrededor del 15 de septiembre de 2017»*.

Los datos expuestos incluyen direcciones de correo electrónico y contraseñas hash para todos los clientes de Cloud WAF que se registraron antes del 15 de septiembre de 2017, así como claves API y certificados SSL proporcionados por el cliente para un subconjunto de usuarios.

*«Activamos nuestro equipo y protocolo interno de respuesta de seguridad de datos, y seguimos investigando con toda la capacidad de nuestros recursos cómo ocurrió esta exposición. Hemos informado a las agencias reguladoras globales apropiadas. Nos hemos comprometido con expertos forenses externos»,* dijo la compañía.

La compañía no ha revelado cómo se filtraron los datos de los clientes de Cloud WAF, si sus servidores se vieron comprometidos o si se dejaron sin seguridad accidentalmente en una base de datos mal configurada en Internet.

Sin embargo, Imperva sigue investigando lo ocurrido, la compañía se ha asegurado de informar a todos los clientes afectados directamente y también está tomando medidas



adicionales para aumentar su seguridad.

*«Lamentamos profundamente que este incidente haya ocurrido y seguiremos compartiendo actualizaciones en el futuro. Además, compartiremos los aprendizajes y las nuevas mejores prácticas que puedan surgir de nuestra investigación y las medidas de seguridad mejoradas con la industria en general», dice la compañía.*

Se recomienda a los usuarios de Cloud WAF que cambien las contraseñas de sus cuentas, implementen Single Sign-On (SSO), habiliten la autenticación de dos factores (2FA), generen y carguen nuevos certificados SSL y restablezcan sus claves API.