Vulnerabilidad En SDN Obligó OpenDaylight A Enfocarse En La Seguridad

Los proyectos de software de código abierto son a menudo bien intencionados, pero la seguridad puede ser dejada de lado en ocasiones.

OpenDaylight, el proyecto de múltiples proveedores de red definida por software (SDN), se enteró de la manera más dura en Agosto pasado después de una vulnerabilidad crítica fue encontrada en su plataforma.

Hubo que esperar hasta diciembre para solucionar la falla, llamada Netdump, el tiempo largo se debió a que el proyecto no contaba con su propio equipo de seguridad dedicado . Gregory Pickett, después de descubrir la vulnerabilidad, publicó en Bugtraq, una lista de correo popular para los fallos de seguridad.

Aunque **OpenDaylight** se encuentra todavía en las primeras etapas y por lo general no se utiliza en entornos de producción, la situación dio importancia a la necesidad de poner un proceso de seguridad en el proyecto.

> *«En realidad es un problema sorprendentemente común con los proyectos de código abierto», dijo **David Jorm**, un ingeniero de seguridad de producto con IIX que formó equipo de respuesta de seguridad de OpenDaylight. «Si no hay personas con un fuerte fondo de seguridad, es muy común que no van a pensar en proporcionar un mecanismo para vulnerabilidades de informes.»*

El proyecto OpenDaylight fue lanzado en abril de 2013 y con el apoyo de proveedores como **Cisco Systems, IBM, Microsoft,**

Ericsson y VMware. El objetivo es desarrollar productos de red que eliminen componentes innecesarios para la comunicación, lo cual es altamente llamativo para las grandes empresas.

La seguridad será un **componente integral de la SDN,** ya que un error podría tener consecuencias devastadoras. Por comprometer un controlador, un componente crítico SDN dicen a los interruptores cómo deben reenviar los paquetes de datos al atacante, ha mencionado Jorm.

«Es un objetivo muy alto valor para ir después», dijo Jorm.

La falla Netdump pateó OpenDaylight en acción, y ahora hay un equipo de seguridad en el lugar de una serie de proveedores que representan diferentes proyectos dentro OpenDaylight, dijo Jorm.

El comité de gestión técnica de OpenDaylight también aprobó recientemente un proceso de respuesta de seguridad detallando el modelo en uno utilizado por la **Fundación OpenStack**, dijo Jorm.