En otro caso de ataque a la cadena de suministro de sofware, decenas de temas y plugins de WordPress alojados en el sitio web de un desarrollador fueron hackeados con código malicioso en la primera quincena de septiembre de 2021, con el objetivo de infectar más sitios.

La puerta trasera les dio a los atacantes el control administrativo total sobre los sitios web que usaban 40 temas y 53 complementos pertenecientes a AccessPress Themes, una compañía con sede en Nepal que cuenta con no menos de 360 mil instalaciones activas de sitios web.

> *«Las extensiones infectadas contenían un cuentagotas para un shell web que brinda a los atacantes acceso completo a los sitios infectados. Las mismas extensiones estaban bien si se descargaban o instalaban directamente desde el directorio de WordPress[.]org»,* dijeron los investigadores de JetPack, un desarrollador de la suite de complementos de WordPress.

Se le asignó el identificador CVE-2021-24867 a la vulnerabilidad en cuestión. La plataforma de seguridad de sitios web Sucuri, en un análisis separado, dijo que algunos de los sitios web infectados encontrados utilizando esta backdoor tenían cargas útiles de spam que se remontan a casi tres años, lo que implica que los actores detrás de la operación estaban vendiendo acceso a los sitios a operadores de otras campañas de spam.

A inicios del mes, la compañía de seguridad cibernética eSentire, reveló cómo los sitios web de WordPress comprometidos que pertenecen a empresas legítimas se utilizan como semillero para la entrega de malware, sirviendo a los usuarios desprevenidos que buscan acuerdos prenupciales o de propiedad intelectual en motores de búsqueda como Google con un implante llamado GootLoader.

Se recomienda a los propietarios de sitios web que hayan instalado los plugins directamente desde el sitio web de AccessPress Themes, que actualicen inmediatamente a una versión segura o que la reemplacen con la última versión de WordPress. Además, se requiere una

implementación de una versión limpia de WordPress para revertir las modificaciones realizadas durante la instalación de la backdoor.

Los hallazgos también se producen cuando la compañía de seguridad de WordPress, Wordfence, reveló los detalles de una vulnerabilidad de secuencias de comandos entre sitios (XSS) ahora parcheada, que afecta a un complemento llamado «WordPress Email Template Designer – WP HTML Mail«, que está instalado en más de 20 mil sitios web.

La vulnerabilidad, rastreada como CVE-2022-0218, se calificó con 8.3 en el sistema de calificación de vulnerabilidades CVSS y se solucionó como parte de las actualizaciones publicadas el 13 de enero de 2022 (versión 3.1).

> *«Esta falla hizo posible que un atacante no autenticado inyectara JavaScript malicioso que se ejecutaría cada vez que un administrador del sitio accediera al editor de plantillas. Esta vulnerabilidad también les permitiría modificar la plantilla de correo electrónico para que contenga datos arbitrarios que podrían usarse para realizar un ataque de phishing contra cualquier persona que reciba correos electrónicos del sitio comprometido»*, dijo Chloe Chamberland.

Según las estadísticas publicadas por Risk Based Security este mes, se descubrieron e informaron alrededor de 2240 fallas de seguridad en complementos de WordPress de terceros hacia finales de 2021, un 142% más que en 2020, cuando se revelaron casi 1000 vulnerabilidades. Hasta ahora, se han descubierto un total de 10359 vulnerabilidades de plugins de WordPress.