09.12.2020
DIVISIÓN DE REDES DE SEGURIDAD INFORMÁTICA
DEPARTAMENTO CSIRT

COMUNICADO SOBRE EL ACCESO NO AUTORIZADO A LAS HERRAMIENTAS DE RED TEAM DE FIREEYE

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información liberada por FireEye sobre el acceso no autorizado a las herramientas de su Red Team por parte de un actor de amenazas altamente sofisticado.

Según la investigación, se detectó que accedieron a ciertas herramientas de Red Team que se utiliza para evaluar la seguridad de sus clientes. Por esa razón se han desarrollado más de 300 contramedidas de detección, con el fin de que puedan ser utilizadas para minimizar el impacto potencial del robo de estas herramientas, disponibles en el siguiente enlace: https://github.com/fireeye/red_team_tool_countermeasures

El presente comunicado tiene como objetivo recordarle a los administradores de los sistemas mantener los sistemas informáticos actualizados. Además, compartimos la lista priorizada de CVE que deben abordarse para limitar la efectividad de las herramientas Red Team y, en algunos casos, sus respectivas mitigaciones en los informes publicados por el CSIRT.

1. **CVE-2020-1472:** Escalada de privilegios de Microsoft Active Directory - CVSS 10.0
2. **CVE-2020-0688:** Ejecución remota de comandos en Microsoft Exchange - CVSS 8.8
3. **CVE-2018-13379:** Lectura de archivos arbitrarios de autenticación previa desde Fortinet Fortigate SSL VPN - CVSS 9.8
4. **CVE-2019-0708:** RCE de los servicios de escritorio remoto de Windows (RDS) - CVSS 9.8
5. **CVE-2019-19781:** RCE de Citrix Application Delivery Controller y Citrix Gateway: CVSS 9.8
6. **CVE-2019-11510:** Lectura de archivos arbitrarios previa a la autenticación de las VPN SSL de Pulse Secure - CVSS 10.0
7. **CVE-2018-15961:** RCE a través de Adobe ColdFusion (carga de archivo arbitrario que se puede usar para cargar un shell web JSP) - CVSS 9.8
8. **CVE-2019-0604:** RCE para Microsoft Sharepoint - CVSS 9.8
9. **CVE-2019-11580:** Ejecución remota de código de Atlassian Crowd - CVSS 9.8
10. **CVE-2020-10189**: RCE para ZoHo ManageEngine Desktop Central - CVSS 9.8
11. **CVE-2014-1812:** Escalamiento de privilegios locales de Windows - CVSS 9.0
12. **CVE-2019-3398:** Ejecución remota de código autenticado por Confluence - CVSS 8.8
13. **CVE-2016-0167:** Escalamiento de privilegios local en versiones anteriores de Microsoft Windows - CVSS 7.8
14. **CVE-2017-11774:** RCE en Microsoft Outlook a través de la ejecución de documentos diseñados (phishing) - CVSS 7.8
15. **CVE-2018-8581**: Escalada de privilegios de Microsoft Exchange Server - CVSS 7.4
16. **CVE-2019-8394:** Carga arbitraria de archivos de autorización previa a ZoHo ManageEngine ServiceDesk Plus - CVSS 6.5

Junto con esto, se recomienda revisar las publicaciones del blog de FireEye para obtener más información:

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2020.12.09
19:24:12 -03'00'