Alerta de seguridad informática	9VSA-00032-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2019
Última revisión	11 de agosto de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por FORTINET referente vulnerabilidades que afectan a varios de sus productos, así como las actualizaciones asociadas liberadas por el proveedor.

Vulnerabilidad

CVE-2018-13379
CVE-2018-13380
CVE-2018-13381
CVE-2018-13382
CVE-2018-13383

Impacto

CVE-2018-13379

Una vulnerabilidad de recorrido transversal en el portal web FortiOS SSL VPN puede permitir que un atacante no autenticado descargue archivos del sistema FortiOS mediante solicitudes de recursos HTTP especialmente diseñadas.

Productos Afectados

- FortiOS 5.6.3 a 5.6.7
- FortiOS 6.0.0 a 6.0.4, solo si el servicio VPN SSL (modo web o modo túnel) está habilitado.

Mitigación

Actualice a FortiOS 5.6.8, 6.0.5 o 6.2.0
Alternativamente, y como solución temporal, se puede deshabilitar completamente el servicio SSL-VPN (tanto en modo web como en modo túnel) aplicando los siguientes comandos:

- config vpn ssl settings
- unset source-interface
- end

El proveedor pide que se tenga en consideración que las políticas del firewall vinculadas a SSL VPN deberán ser desactivadas antes para que la secuencia anterior se ejecute con éxito.

Enlace
https://fortiguard.com/psirt/FG-IR-18-384

Impacto

CVE-2018-13380

Se detectaron múltiple vulnerabilidad XSS previas a la autenticación en SSL VPN. Si no se desinfectan los parámetros de error o manejo de mensajes en el portal web SSL VPN, un atacante puede realizar un ataque de Cross-site Scripting (XSS).

Productos Afectados

- FortiOS 6.0.0 to 6.0.4
- FortiOS 5.6.0 to 5.6.7
- FortiOS 5.4 y anteriores

Mitigación

Actualice a FortiOS 5.6.8, 6.0.5 o 6.2.0
Alternativamente, en versiones no fijadas, si la función del portal web SSL-VPN está habilitada, deshabilite el servicio del portal web SSL-VPN aplicando los siguientes comandos:
Para FortiOS 5.0 y anteriores:

- config vpn ssl settings
- set sslvpn-enable disable
- end

Para FortiOS 5.2 y siguientes:

- config vpn ssl settings
- unset source-interface
- end

Enlace
https://fortiguard.com/psirt/FG-IR-18-383

Impacto

CVE-2018-13381

Se detectó que el búfer se desborda a través de la carga útil del mensaje POST. Si no analiza correctamente las cargas de mensajes en el portal VPN SSL de FortiOS, puede permitir que un atacante no autenticado realice un ataque de denegación de servicio mediante la explotación de un desbordamiento de búfer.

Productos Afectados

FortiOS 6.0.0 a 6.0.4
FortiOS 5.6.0 a 5.6.7
FortiOS 5.4 y anteriores

Mitigación

Actualice a FortiOS 5.6.8, 6.0.5 o 6.2.0
Deshabilite el servicio del portal web SSL-VPN aplicando los siguientes comandos:
Para FortiOS 5.0 y anteriores:

- config vpn ssl settings
- set sslvpn-enable disable
- end

Para FortiOS 5.2 y siguientes:

- config vpn ssl settings
- unset source-interface
- end

Enlace
https://fortiguard.com/psirt/FG-IR-18-387

Impacto

CVE-2018-13382

Una vulnerabilidad de autorización incorrecta en el portal web SSL VPN puede permitir que un atacante no autenticado cambie la contraseña de un usuario del portal web SSL VPN a través de solicitudes HTTP especialmente diseñadas.

Productos Afectados

FortiOS 6.0.0 a 6.0.4
FortiOS 5.6.0 a 5.6.8
FortiOS 5.4.1 a 5.4.10
Solo si el servicio VPN SSL (modo web o modo túnel) está habilitado.

Se debe considerar que solo los usuarios con autenticación local se ven afectados. Esto afecta a usuarios con autenticación remota (LDAP o RADIUS).
Las versiones 5.4.0 y anteriores (incluida la rama 5.2) no se ven afectadas.

Mitigación

Actualice a FortiOS 5.4.11, 5.6.9, 6.0.5, 6.2.0 o superior.
La única solución alternativa es migrar la autenticación de usuario SSL VPN de local a remota (LDAP o RADIUS), o deshabilitar totalmente el servicio SSL-VPN (tanto en modo web como en modo túnel) aplicando los siguientes comandos:

- config vpn ssl settings
- unset source-interface
- end

Tenga en cuenta que las políticas de firewall vinculadas a SSL VPN deberán ser desactivadas primero para que la secuencia anterior se ejecute con éxito.

Enlace
https://fortiguard.com/psirt/FG-IR-18-389

Impacto

CVE-2018-13383

Una vulnerabilidad de desbordamiento del búfer de almacenamiento dinámico en el portal web FortiOS SSL VPN puede provocar la finalización del servicio web SSL VPN para los usuarios registrados o la posible ejecución remota de código en FortiOS. Esto sucede cuando un usuario autenticado visita una página web de edición proxy específicamente diseñada, y esto se debe a una falla en el manejo adecuado del contenido href de JavaScript. Esto solo afecta el modo web SSL VPN (el modo túnel SSL VPN no se ve afectado). La falla podría ser explotada en un ataque de Denegación de Servicio ejecutado por código remoto.

Productos Afectados

FortiOS 6.0.0 a 6.0.4
FortiOS 5.6.0 a 5.6.8
FortiOS 5.4.1 a 5.4.10
Solo si el servicio VPN SSL (modo web o modo túnel) está habilitado.
Se debe considerar que solo los usuarios con autenticación local se ven afectados. Esto afecta a usuarios con autenticación remota (LDAP o RADIUS).
Las versiones 5.4.0 y anteriores (incluida la rama 5.2) no se ven afectadas.

Mitigación

Actualice a FortiOS 6.0.5 o 6.2.0
Alternativamente puede utilice solo el modo de túnel VPN SSL

Otra recomendación es acceder solo a servidores web HTTP confiables en modo web VPN SSL
También puede deshabilitar totalmente el servicio SSL-VPN aplicando los siguientes comandos:

- config vpn ssl settings
- unset source-interface
- end

Enlace
https://fortiguard.com/psirt/FG-IR-18-388

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.11 13:44:52 -04'00'