Incidencia de vulnerabilidad

Organizacion	COPA
Fecha	Marzo 21, 2018
Servicio	MSS-VME
Seguridad nivel	Medium
Impacto Nivel	Medium
Vulnerabilidad Nivel	Medium

SSL /TLS Protocol Initialization Vector Implementación Información disclosure

Existe una vulnerabilidad en SSL 3.0 y TLS 1.0 que podría permitir la divulgación de información si un atacante intercepta el tráfico cifrado servido desde un sistema afectado. TLS 1.1, TLS 1.2 y todas las suites de cifrado que no usan el modo CBC no se ven afectadas

Solución

Configure los servidores SSL / TLS para que solo utilicen TLS 1.1 o TLS 1.2 si es compatible. Configure los servidores SSL / TLS para que solo sean compatibles con suites de cifrado que no usan cifras de bloque. Aplique los parches si están disponibles.

Sistemas Afectados

443 / tcp / cisco-ssl-vpn-svr 201.218.212.9, 201.218.212.35
443 / tcp / www 200.46.240.137,ec2-52-3-92-27.compute1.amazonaws.com,ec2-52-72-43-239.compute-1.amazonaws.com,ec2-54-164-239-210.compute-1 .amazonaws.com
443 / tcp / elasticsearch ec2-52-86-152-128.compute-1.amazonaws.com

Elasticsearch Unrestricted Access Information Disclosure

La aplicación Elasticsearch que se ejecuta en el servidor web remoto se ve afectada por una vulnerabilidad de divulgación de información debido a la imposibilidad de restringir los recursos mediante la autenticación

Impacto

Un atacante remoto no autenticado puede explotar esto para divulgar información confidencial de la base de datos.

Salida

GLESEC detectó una instancia desprotegida de Elasticsearch con los siguientes índices:
.kibana

Usuarios

Solución

Habilite la autenticación de usuarios nativos o integre con un sistema de administración

de usuarios externo como LDAP y Active Directory.

Sistemas Afectados

443 / tcp / elasticsearch	ec2-52-86-152-128.compute-1.amazonaws.com
80 / tcp / elasticsearch	ec2-52-86-152-128.compute-1.amazonaws.com

Vulnerabilidad relacionada con SSL/TLS (implementados en la aplicación Open SSL)

Se consideran inseguras aquellas suites de cifrado que utilicen los algoritmos de cifrado DES, 3DES e IDEA y el algoritmo de hash SHA-1.

Solución

GLESEC, recomienda eliminar de la suite todas las entradas relacionadas con los algoritmos
mencionados.

Sistemas Afectados

443 / tcp / cisco-ssl-vpn-svr	201.218.212.9
443 / tcp / www	200.46.240.137

Web Server Generic XSS

El host remoto está ejecutando un servidor web que no puede desinfectar adecuadamente las cadenas de solicitud de JavaScript malicioso.

Impacto

Un atacante remoto puede explotar este problema, a través de una solicitud especialmente diseñada, para ejecutar código HTML y de script arbitrario en el navegador de un usuario dentro del contexto de seguridad del sitio afectado.

Solución

Genere un parche o una actualización

Salidas

```
The request string used to detect this flaw was:

/<script>cross_site_scripting.nasl</script>.asp

The output was:

HTTP/1.1 405 Method Not Allowed
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8
Content-Length: 138
Connection: keep-alive
{"error":"Incorrect HTTP method for uri [/<script>cross_site_scripting.n
asl</script>.asp] and method [GET], allowed: [POST]","status":405}


Note that this XSS attack may only work against web browsers
```

that have "content sniffing" enabled.

Sistemas Afectados

443 / tcp / elasticsearch	ec2-52-86-152-128.compute-1.amazonaws.com
80 / tcp / elasticsearch	ec2-52-86-152-128.compute-1.amazonaws.com

Nota: GLESEC, recomienda aplicar estas recomendaciones a la BREVEDAD posible, a fin de mitigar el riesgo de explotación de estas vulnerabilidades.

Estamos atentos ante cualquier duda o inquietud de su parte.

Saludos Cordiales,

GLESEC OPERATION CENTER – GOC.