BOLETÍN DE ALERTA

Boletín Nro.: 2017-03
Fecha de publicación: 21/04/2017
Tema: Vulnerabilidad de Ejecución Remota de Código en Squirrelmail

Sistemas afectados:

- Squirrelmail 1.4.22 y versiones previas

Descripción:

Se ha reportado una vulnerabilidad crítica de ejecución remota de código que afecta al popular software de correo Squirrelmail, versión 1.4.22 y previas, debido a una falla en la sanitización de la cadena que es pasada como argumento a la llamada popen.

La vulnerabilidad se encuentra en el archivo Deliver_SendMail.class.php, en la función initStream, la cual utiliza una función de escapado inadecuada, escapeshellcmd(), la cual no escapa los espacios, permitiendo de esta manera la inyección de comandos arbitrarios a través de la variable $envelopefrom, la cual puede ser construida de tal manera a inyectar un archivo de configuración que dispare la ejecución arbitraria de código.

```
95          // Save executed command for future reference
96          $this->sendmail_command = "$sendmail_path $this->sendmail_args -f$envelopefrom";
97          // open process handle for writing
98          $stream = popen(escapeshellcmd($this->sendmail_command), "w");
99          return $stream;
```

La vulnerabilidad es explotable en aquellos servidores en los que el MTA utilizado es sendmail y si Squirelmail está configurado de tal manera a utilizarlo como commandline, es decir, si la directiva useSendmail del archivo de configuración está en True, una configuración relativamente frecuente en instalaciones de Squirrelmail.

Un atacante puede explotar esta vulnerabilidad de modo a ejecutar comandos de shell arbitrarios de forma remota en el servidor.

Se han asignado dos CVE a dicha vulnerabilidad, CVE-2017-5181 y CVE-2017-7692 sin embargo, está en proceso de revisión para fusionarlos en uno solo. Dos investigadores han descubierto la vulnerabilidad de forma independiente y han contactado al desarrollador de Squirrelmail, sin embargo, éste no ha podido responder hasta la fecha. Igualmente, se han publicado exploits funcionales. Debido a la falta de

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

parche oficial para dicha vulnerabilidad, los investigadores han publicado un parche no oficial que puede ser aplicado para corregir esta vulnerabilidad.

Impacto

Explotando esta vulnerabilidad un atacante remoto no autorizado podría obtener un control total del servidor que ejecuta la versión vulnerable de Squirrelmail.

Solución

Se puede corregir la vulnerabilidad, reemplazando la línea 96 y 98 del archivo squirrelmail-webmail-1.4.22/class/deliver/Deliver_SendMail.class.php por el siguiente código:

```
$this->sendmail_command = escapeshellcmd("$sendmail_path $this->sendmail_args -f") .
escapeshellarg($envelopefrom);
$stream = popen($this->sendmail_command, "w");
```

Información adicional:

https://www.wearesegment.com/research/Squirrelmail-Remote-Code-Execution.html

http://www.securityfocus.com/archive/1/540438

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py