Investigadores de Cisco Talos descubrieron múltiples vulnerabilidades en la familia de software OpenSIS, un sistema de gestión de información para estudiantes K-12, disponible en versión comercial y de código abierto, que permite a las escuelas crear horarios y realizar seguimiento de asistencia, calificaciones y transcripciones.

Un atacante podría aprovechar las vulnerabilidades para ejecutar varias acciones maliciosas, como la inyección SQL y ejecución remota de código.

Los investigadores descubrieron múltiples vulnerabilidades (CVE-2020-6117, CVE-2020-6118, CVE-2020-6119, CVE-2020-6120, CVE-2020-6121 y CVE-2020-6122) de inyección SQL explotables en la página CheckDuplicateStudent.php de OS4Ed openSIS 7.3. Una solicitud especialmente diseñada conduce a la inyección de SQL.

Estas vulnerabilidades recibieron un puntaje de severidad de 6.4 en la escala CVSS 3.0.

Otras dos vulnerabilidades de inyección SQL (CVE-2020-6123 y CVE-2020-6124), residen en la funcionalidad de parámetros de correo electrónico de OS4Ed openSIS 7.3. Una solicitud HTTP especialmente diseñada puede conducir a una inyección SQL.

Un error de inyección SQL (CVE-2020-6125), puede ser explotable en la funcionalidad GetSchool.php de OS4Ed openSIS 7.3. Esta vulnerabilidad también recibió un puntaje de severiad de 6.4.

Tres vulnerabilidades de inyección SQL (CVE-2020-6126, CVE-2020-6127 y CVE-2020-6128), pueden ser explotables en la funcionalidad GetSchool.php de OS4Ed opensis 7.3.

Según Talos, el 13 de agosto pasado, OpenSIS emitió un parche para estas vulnerabilidades, confirmando la resolución del problema el 17 de agosto.

Otro conjunto de vulnerabilidades (CVE-2020-6129, CVE-2020-6130 y CVE-2020-6131), son explotables para el parámetro course_period_id en la funcionalidad GetSchool.php de OS4Ed openSIS 7.3.

El investigador Yuri Kramarz de Cisco Talos describe los errores en su reporte de vulnerabilidad.

Para el mismo parámetro course_period_id, las vulnerabilidades CVE-2020-6132, CVE-2020-6133 y CVE-2020-6134, permiten que una solicitud HTTP especialmente diseñada pueda conducir a una inyección SQL.

Por otro lado, existe una vulnerabilidad CVE-2020-6135 de inyección SQL en la funcionalidad Validator.php que también requiere una solititud HTTP especialmente diseñada por el atacante.

Otra vulnerabilidad (CVE-2020-6136) para la funcionalidad Validator.php y DownloadWindow.php, permite al atacante inyectar código SQL mediante una función HHTP especialmente diseñada.

Para la funcionalidad de restablecimiento de contraseña de OS4Ed openSIS 7.3, existen múltiples vulnerabilidades (CVE-2020-6137, CVE-2020-6138, CVE-2020-6139 y CVE-2020-6140), que permiten la inyección de código SQL mediante una solicitud HTTP especialmente diseñada.

La vulnerabilidad CVE-2020-6141, de ser explotada, podría permitir la inyección SQL en la funcionalidad de inicio de sesión de OS4Ed openSIS 7.3, de igual forma, mediante una solicitud HTTP especialmente diseñada.

Una vulnerabilidad de ejecución remota de código (CVE-2020-6142) existe en la funcionalidad Modules.php de OS4Ed openSIS 7.3, que mediante una solicitud HTTP especialmente diseñada, puede provocar la inclusión de archivos locales. Esta vulnerabilidad recibió un puntaje de severidad de 9.9.

La vulnerabilidad CVE-2020-6144, permite la ejecución remota de código en la funcionalidad de instalación de OS4Ed openSIS 7.4, mediante una solicitud HTTP especialmente diseñada. Esta vulnerabilidad recibió la puntuación más alta de criticidad de 10 en la escala CVSS.

Se recomienda a los administradores de OpenSIS que apliquen los parches correspondientes inmediatamente.