Vulnerabilidades en PcVue SCADA/HMI

BCSC_ALERTA_Vulnerabilidades_PcVue_SCADA/HMI

TLP:WHITE

www.basquecybersecurity.eus

Noviembre 2020

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

Investigadores de seguridad han publicado varias vulnerabilidades potencialmente graves en la solución PcVue SCADA/HMI, software de monitorización y control industrial, que podrían permitir a un atacante remoto no autenticado llevar a cabo la ejecución de código, acceder a información confidencial y causar interrupciones de servicio.

La investigación ha identificado **tres vulnerabilidades**, una de las cuales ha recibido la calificación de **crítica** al estar relacionada con una deserialización insegura de los mensajes recibidos en la interfaz y podría conducir a la **ejecución remota de código**. Las otras dos vulnerabilidades han sido calificadas con una gravedad alta en base a que una de ellas podría ser aprovechada para realizar **ataques DoS**, mientras que la otra consiste en un problema de divulgación de información que permitiría a un atacante **acceder a datos de sesión de usuarios legítimos**. Según los reportes, la explotación de estos fallos es relativamente fácil y no requiere la interacción de un usuario.

La empresa francesa encargada del desarrollo y mantenimiento de **PcVue**, ARC Informatique, ya ha solucionado estas vulnerabilidades con el lanzamiento de la versión **12.0.17** del producto y ha compartido medidas de mitigación con el fin de prevenir posibles ataques. Además, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) también ha hecho público un aviso advirtiendo a las organizaciones de los riesgos que plantean estos fallos.

ANÁLISIS TÉCNICO

Se han publicado varias vulnerabilidades que afectan a **PcVue,** software orientado al control de entornos industriales que incorpora las últimas funciones de interfaz de usuario de **Microsoft** y las funciones de seguridad de las plataformas **Windows**. El producto cumple con los estándares industriales de confiabilidad y rendimiento y es capaz de administrar aplicaciones de un solo usuario, como aplicaciones cliente-servidor o de cliente ligero del tipo HTML5 Web y ofrece la posibilidad de implementar arquitecturas redundantes virtualizadas y de alta disponibilidad.

A continuación, se exponen los detalles técnicos sobre las tres vulnerabilidades detectadas:

- **CVE-2020-26867**: PcVue en sus versiones anteriores a la 12.0.17 contiene una vulnerabilidad debida a una deserialización de datos que no son de confianza, al no verificar suficientemente que los datos resultantes sean válidos, lo que puede permitir a un atacante **ejecutar código de forma remota** en la web y el servidor *back-end* móvil.

  La vulnerabilidad ha recibido un score de **9.8** según la escala **CVSSv3.1**, es decir, se trata de un error crítico ya que es explotable de forma remota, con una complejidad baja y sin requerir privilegios ni interacción por parte de un usuario.

- **CVE-2020-26868**: PcVue en sus versiones anteriores a la 12.0.17 es vulnerable a un ataque de **denegación de servicio (DoS)** debido a la posibilidad que tiene un usuario no autorizado de modificar la información utilizada para validar los mensajes enviados por clientes web legítimos. El problema también afecta a sistemas de terceros basados en *Web Services Toolkit*.

  Si un atacante logra modificar una variable para que contenga valores inesperados, provocaría alteraciones en las suposiciones de otras partes del código. Además, en caso de llegar a leer una variable privada, podría exponer información confidencial o facilitar el lanzamiento de más ataques.

- **CVE-2020-26869**: PcVue en sus versiones anteriores a la 12.0.17 es vulnerable a una posible **exposición de información no autorizada**, lo que permitiría a usuarios no autorizados acceder a datos de sesión de usuarios legítimos. Al igual que la vulnerabilidad anterior, este problema también afecta a sistemas de terceros basados en *Web Services Toolkit*.

Las dos últimas vulnerabilidades han recibido un score de **7.5** según la escala **CVSSv3.1**, es decir, son errores con una gravedad alta ya que son explotables de forma remota, con una complejidad baja y sin requerir privilegios ni interacción por parte de un usuario.

Hasta la fecha, no se conocen reportes de posibles explotaciones activas en la red o la disponibilidad de exploits o pruebas de concepto para estas tres vulnerabilidades.

Tal y como se ha mencionado en la descripción de cada vulnerabilidad las versiones afectadas de **PcVue** son, concretamente, desde la **8.10**, incluida, hasta la **12.0.17**, sin incluir.

MITIGACIÓN / SOLUCIÓN

ARC Informatique ya ha lanzado la versión **12.0.17** de **PcVue** que solventa estos errores, por lo que la solución pasa por aplicar esta actualización poniéndose en contacto con el servicio de asistencia de PcVue para recibir instrucciones sobre la descarga e instalación de la última versión del software.

Al margen la actualización descrita anteriormente, el fabricante recomienda implementar las siguientes medidas de mitigación con el fin de reducir el riesgo de sufrir posibles ataques:

- Desinstalar los componentes afectados *backend web* y móvil en los terminales de los usuarios que no los utilicen o no les sean necesarios.
- En versiones anteriores a la 12.0.* se recomienda modificar la configuración predeterminada del *backend web* y móvil. Dicha modificación deberá efectuarse de forma manual cambiando el siguiente elemento de configuración para evitar la ejecución remota de código:

  En el archivo ***<PcVue installation directory>\Bin\PropertyServer.config>***, establecer el siguiente elemento en "Low" (por defecto en "Full"):

  ```
  <serverProviders>
      <formatter ref="binary" typeFilterLevel="Low" />
  </serverProviders>
  ```

- Fortalecer la configuración del firewall asegurándose de que las conexiones entrantes en el puerto correspondiente sólo se autorizan si se inician mediante el proceso del servidor web de IIS. El puerto de escucha es configurable (por defecto 8090) y puede haberse cambiado en el sistema utilizando el Explorador de aplicaciones.

Adicionalmente, es recomendable adoptar las siguientes medidas defensivas de carácter más general con el fin de reducir al mínimo el riesgo de explotación de estas vulnerabilidades:

- Minimizar la exposición a la red de todos los dispositivos y/o sistemas de control, y asegurarse de que no sean accesibles desde Internet.
- Localizar las redes de sistemas de control y los dispositivos remotos detrás de los firewalls, y aislarlos de la red de la organización.
- Cuando se requiera el acceso remoto, utilizar métodos seguros, como las redes privadas virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible.

REFERENCIAS ADICIONALES

- PcVue Solutions - 3 vulnerabilities affect the interface between the Web & Mobile back end and the web services hosted in Microsoft IIS
- KLCERT-20-015: Remote Code Execution in ARC Informatique PcVue
- KLCERT-20-016: Denial-of-Service in ARC Informatique PcVue
- KLCERT-20-017: Session Information Exposure in ARC Informatique PcVue
- ICS Advisory (ICSA-20-308-03) - ARC Informatique PcVue

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?