AVISO DE SEGURIDAD

La Oficina del Comisionado de Seguros de Puerto Rico (OCS) informa al público y a las entidades reguladas sobre un incidente de ciberseguridad reportado por la National Association of Insurance Commissioners (NAIC), organización que provee apoyo técnico y sistemas regulatorios utilizados por reguladores de seguros en los Estados Unidos y sus territorios.

Según la información oficial emitida por la NAIC, el 11 de junio de 2026 se identificó un acceso no autorizado a una porción limitada de su infraestructura tecnológica, relacionado con una vulnerabilidad de día cero (*zero-day vulnerability*) en la plataforma Oracle PeopleSoft. El incidente fue contenido de forma inmediata y actualmente se encuentra bajo investigación con el apoyo de expertos en ciberseguridad y en coordinación con el Federal Bureau of Investigation (FBI). Conforme a los hallazgos preliminares:

- No se comprometió información personal identificable (PII), incluyendo números de seguro social, información bancaria, tarjetas de crédito u otra información de pago sensitiva.
- Los sistemas utilizados por los departamentos y oficinas regulatorias estatales y territoriales no fueron comprometidos.
- Tampoco fueron afectados sistemas regulatorios críticos, incluyendo:
    - System for Electronic Rate and Form Filing
    - Online Premium Tax for Insurance
    - Uniform Certificate Authority Application
    - Enterprise Data Platform
    - Regulatory Data Collection
    - National Insurance Producer Registry
    - State Based Systems

La información a la que presuntamente se tuvo acceso consistió principalmente en ciertos datos financieros regulatorios y determinada información relacionada con agencias de clasificación crediticia. Sin embargo, la NAIC ha indicado que, hasta este momento, no existe confirmación de publicación o divulgación de información extraída.

La OCS se mantiene en comunicación con la NAIC y continuará monitoreando el desarrollo de este incidente. Reiteramos nuestro compromiso con la protección de la información y la continuidad de los servicios regulatorios esenciales, manteniendo informados al público y a las entidades reguladas sobre cualquier desarrollo relevante.

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Security Incident Fact Sheet

June 23, 2026, as of 3:15 p.m. ET

This information reflects the NAIC's current understanding based on the facts developed to date. Updates will be posted to NAIC.org as they are available.

Incident Background

- Unauthorized access to a portion of the NAIC's environment was identified on June 11 via an Oracle PeopleSoft vulnerability. While in PeopleSoft, the unauthorized party was able to obtain information needed to gain temporary access to certain data storage areas. The ability to gain this temporary access has been blocked and remediated.
- The incident was promptly contained following detection, and the NAIC engaged outside counsel and cybersecurity experts. FBI coordination is underway.
- The incident resulted from a broad campaign to exploit a vulnerability in PeopleSoft that was unknown to the developer or software users at the time, otherwise known as a "zero-day vulnerability," which affected multiple organizations. The NAIC uses PeopleSoft primarily for internal financial reporting purposes.
- Based on our investigation with outside cybersecurity experts and what we know today, we do not believe the group responsible has the amount or scope of data it has claimed, and as of this writing, we have no confirmation that data from our environment has been published or released.

Impacts

- Data accessed or acquired, based on findings to date, included:
    - Publicly available statutory financial reporting information. These statements were publicly available prior to this incident through state websites, InsData, or resellers.
    - Credit rating agency data, including rating determinations of insurer investments. This does not include any rating agency investment rationale reports.
- Importantly, no PII or payment information was accessed, including credit card or banking information.
- Regarding the status of systems:
    - State insurance departments' systems are not impacted.

- The individual or group responsible claimed to have technology provided by the NAIC, including the System for Electronic Rate and Form Filing (SERFF), Online Premium Tax for Insurance (OPTins), Uniform Certificate Authority Application (UCAA), Enterprise Data Platform (EDP), and Regulatory Data Collection (RDC). Outside cybersecurity experts confirmed the unauthorized party did not take this information, nor compromised these regulatory reporting systems.
- Based on findings to date, the following were also not accessed: NIPR, Teammate, State Based Systems (SBS), employee personal data, electronic funds transfer, risk-based capital data, policyholder information, producer data, and event registration payment information.
- Due to the incident, certain credit rating agencies have paused their data feeds and consequently, the NAIC has temporarily suspended assigning designations to insurer investments.

Remediation & Next Steps

- In conjunction with NAIC senior management, our outside cybersecurity experts have confirmed that affected systems have been remediated, and we have taken additional steps to strengthen our defenses with their partnership.
- Our operations have returned to normal with two exceptions:
  - We are meeting with credit rating providers to provide third-party assurances that our systems are secure, and the NAIC designation process can resume.
  - Online invoice payment via PeopleSoft is not yet available.
- We are working with credit rating agencies and anticipate providing them with third-party verification of our systems, and on any steps they require to restore services.
- If the data is released by the group responsible, we will engage cybersecurity experts to compare our data with what affected systems have been remediated.
- We understand that this process can take months. Though speed is important, accuracy is paramount. Updates regarding that process will be communicated to stakeholders and via updates on NAIC.org.