THREAT BULLETINS

Kronos Private Cloud (KPC) Ransomware Incident Causes Downtime

TLP:WHITE

Dec 13, 2021

On December 13, 2021, Kronos reported a ransomware event impacting Kronos Private Cloud (KPC) instances.

Ultimate Kronos Group (UKG) released a statement that recommends Kronos Private Cloud users implement alternative business continuity protocols given that it may take up to several weeks to restore system availability.

Kronos released the following statement to impacted KPC clients:

> We are reaching out to inform you of a cyber security incident that has disrupted the Kronos Private Cloud.

> As we previously communicated, late on Saturday, December 11, 2021, we became aware of unusual activity impacting UKG solutions using Kronos Private Cloud. We took immediate action to investigate and mitigate the issue, and have determined that this is a ransomware incident affecting the Kronos Private Cloud—the portion of our business where UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions are deployed. At this time, we are not aware of an impact to UKG Pro, UKG Ready, UKG Dimensions, or any other UKG products or solutions, which are housed in separate environments and not in the Kronos Private Cloud.
>
> We are working with leading cyber security experts to assess and resolve the situation, and have notified the authorities. The investigation remains ongoing, as we work to determine the nature and scope of the incident.
>
> While we are working diligently, our Kronos Private Cloud solutions are currently unavailable. Given that it may take up to several weeks to restore system availability, we strongly recommend that you evaluate and implement alternative business continuity protocols related to the affected UKG solutions. Support is available via our UKG Kronos Community and via our UKG Customer Support Team to provide input on your business continuity plans.
>
> We deeply regret the impact this is having on you, and we are continuing to take all appropriate actions to remediate the situation. We recognize the seriousness of this issue and will provide another update within the next 24 hours.

Health-ISAC will continue to monitor the situation to determine any additional impact.

An initial public consensus is that on-premises instances are not impacted. Only Kronos Private Cloud (KPC) instances are impacted by the aforementioned ransomware event.

Kronos is a workforce management and human resources provider who provides cloud-based solutions for managing timekeeping, payroll, employee benefits, analytics, and more. In 2020, Kronos merged with Ultimate Software to create a new company named UKG. UKG describes Kronos Private Cloud (KPC) as a secure storage and server facility hosted at third-party data centers. This infrastructure is used to host their Workforce Central, Workforce

TeleStaff, TeleTime IP, Enterprise Archive, Extensions for Healthcare (EHC), and FMSI environments.

According to Kronos, KPC is secured using firewalls, multi-factor authentication, and encrypted transmissions to prevent unauthorized access to their systems. The exact nature of how actors breached the internal systems of UKG remains unknown, but UKG has stated that systems could be unavailable for several weeks as the recovery systems progresses. During this time, UKG suggests customers evaluate and implement alternative business continuity protocols related to the affected solutions.

Reference(s)	The Register, Bleeping Computer, kronos

Sources
The Register: Timekeeping Biz Kronos Hit by Ransomware and Warns Customers to Engage Biz Continuity Plans

Kronos Community: Communications Sent to Impacted Kronos Private Cloud (KPC) Customers Beginning December, 13 at 12:45AM ET

Bleeping Computer: Kronos Ransomware Attack May Cause Weeks of HR Solutions Downtime

Alert ID bf85748f

View Alert

Tags UKG, Kronos Private Cloud, Ransomware Shutdown, Ransomware Alert, Kronos, Ransomware Actors, Ransomware Attacks


For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.