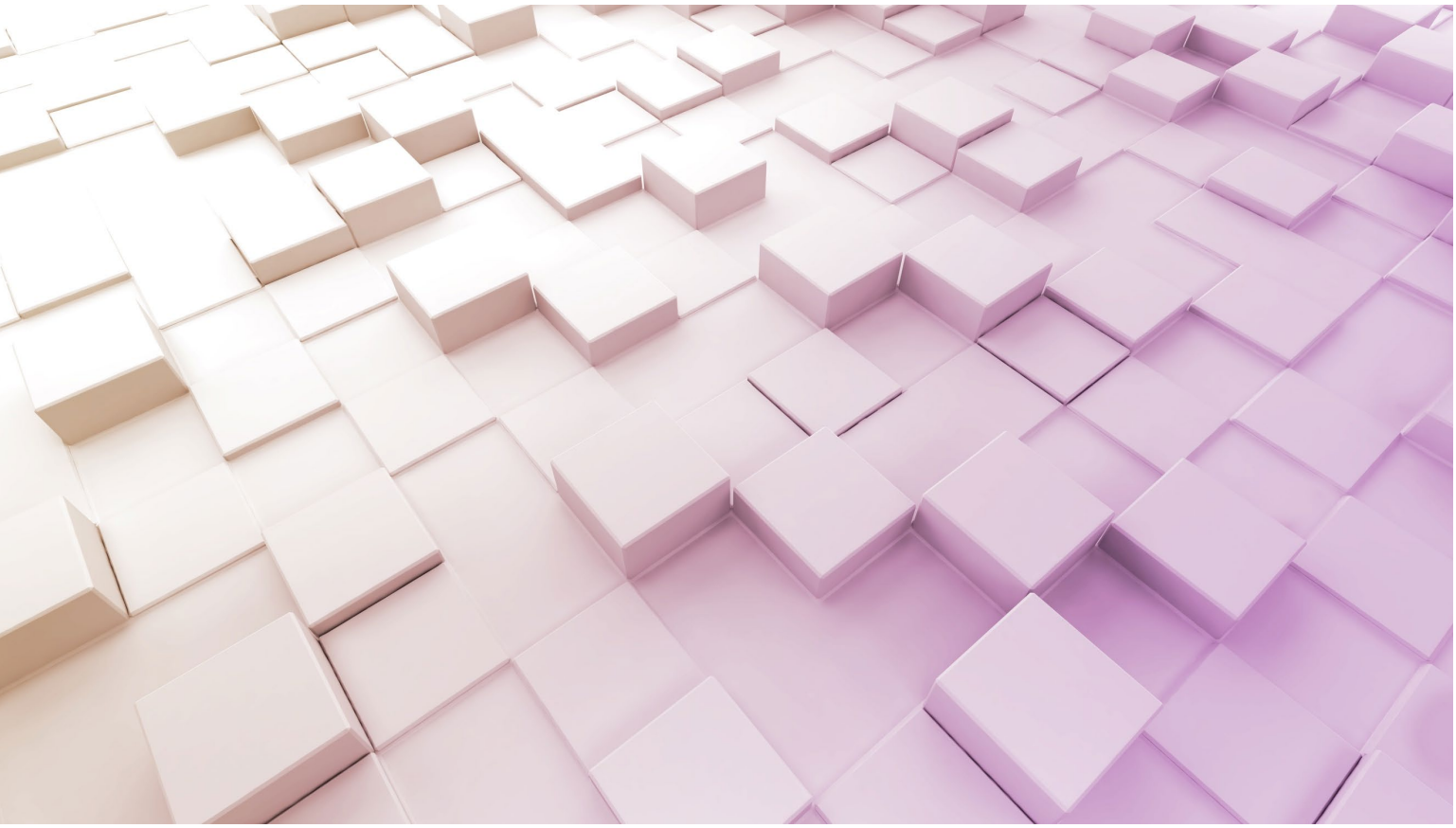


KRONOS DATA BREACH

Recommendations for affected organizations

CYTEX™

Kronos Data Breach

Kronos ransomware incident

Kronos (UKG) is a popular cloud-based HR software application. On December 11, 2021, Kronos communicated to its clients that it "became aware of unusual activity in impacting UKG solutions using Kronos Private Cloud". The company confirmed: "[T]his 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".

This incident has impacted time management, payroll processing, and HR functions of many organizations both in the private and government sector. This incident resulted in a denial-of-service attack on the Kronos customers, who are unable to pay their employees, account for task related hours, and perform other HR tasks that are common at the end of the year. Besides the denial of service, Kronos customers should assume that their employee Personally Identifiable Information (PII) may be compromised leading to identity theft and privacy disclosures.

What happened?

There is limited information on what caused the data breach that led to the ransomware attack. Since this was limited to the Kronos private cloud, we can speculate that it could have resulted from a misconfigured application that was exploited through Log4j [CVE-2021-44228].[1]

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

What should organizations do now?

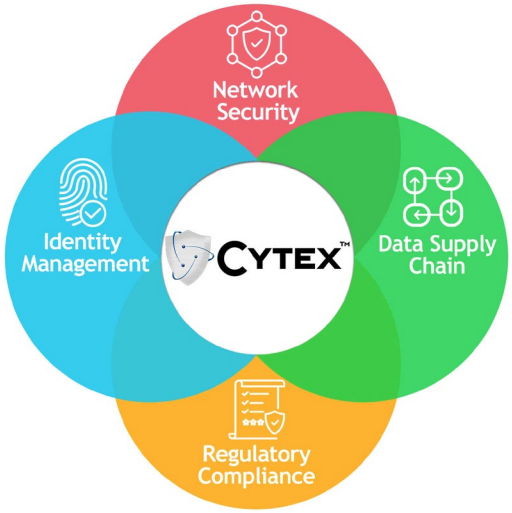
There are several steps organization can take now to mitigate the impact of this incident.

1. Identify a backup plan to switch critical HR functions to paper or transition to another vendor.
2. Communicate with employees.
    a. Ask employees to be vigilant about any suspicious activity that involves changes to their credit, bank accounts, or retirement accounts
    b. Encourage them to sign up for credit monitoring services
3. Review your Kronos service agreement to determine the impact of this incident.
    a. Identify what information is retained by Kronos, how it is stored, and the retention time frame.
    b. Review the contingency clauses to ascertain the outlined process for handling data incidents and the liabilities of each party.
    c. Determine the service outage reimbursements due to the denial of service.
4. Review your cyber insurance policy.
    a. Find out what remedial actions might be covered by your insurance policy.
    b. Insurance policy may cover credit monitoring services and data portability to a different vendor.
5. Perform a cyber assessment on your data supply chain
    a. Identify all your data exchange partners as well as vendors who have access to your data assets.
    b. Evaluate all your vendors to identify your data supply chain risk. Organizations can use the NIST CSRM framework to stratify vendors by risk, impact, and dependency[2]. These audits can be conducted by the organization or collaboratively with each vendor.
    c. Run a vulnerability scan on your data partners and check if there are exploitable vulnerabilities.
    d. Look for known exploits that may exist on the dark web or other malicious sites.

[2] https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

e. Evaluate the Service Level Agreements for each vendor and determine their backup plans in case of a ransomware or data breach incident.
f. Evaluate all your (cloud hosted and on-premises) data assets. Turn on continuous compliance checks to identify at-risk or misconfigured applications.
g. Consider performing a SOC-2 audit on your data assets.
h. Ask for a SOC-2 audit report from your vendors. If they have not performed a SOC-2 audit, encourage your most important data exchange partners to conduct a SOC-2 assessment.

6. Determine if any data breach laws would apply.
    a. If the incident involves disclosure of Personally Identifiable Information, then data breach laws may apply, and the organization would need to comply with the disclosure requirements. If an organization is using Kronos in the European Union, then it may also be subjected to GDPR data disclosure and reporting requirements.
7. Develop a cybersecurity awareness program.
    a. Organizations should use this incident to bolster their existing cybersecurity awareness program.
    b. Develop a culture of awareness that cybersecurity is everyone's responsibility.
    c. Train employees to identify phishing attacks through simulated training programs.
    d. Institute an ongoing vigilance and compliance posture to continuously audit vendors, application configurations, and apply critical patches.
8. Come up with a contingency plan.
    a. Data breach and ransomware incidents are now widespread, and organizations should put remedial plans to deal with any future incidents.
    b. Evaluate disaster recovery, business continuity, and backup plans. Perform a disaster recovery exercise to simulate a data outage and verify the business continuity plan.
    c. Develop a ransomware plan that includes contingency plans for uninterrupted operations, law enforcement contacts, and ransomware payments.
9. Team up Cytex and deploy a unified cybersecurity platform to identify, protect, and defend against future incidents.



Take the first steps towards becoming a cyber resilient organization and contact the Cytex team to get started.

Cytex is a unified resilience platform developed to address the cybersecurity challenges faced by SMBs. Cytex team realizes that SMBs want to grow their business while protecting their valuable data assets against ransomware, cyberattacks, and data breaches. As a unified platform, Cytex provides all the cyber capabilities that enable SMBs to focus on their core business while reducing cost, complexity, and vendor sprawl.

With Cytex, organizations can inventory data exchange partners, conduct CVE indexed vulnerability scans, get cyber threat intelligence, assess cloud and on premise security of applications, perform SOC-2, HIPAA, NIST CSF, PCI, CCPA, GDPR assessments, and manage the security of a hybrid workforce.

https://cytex.io

hello@cytex.io

@cytexsmb

https://bit.ly/3sEZhJr