UKG Hack Disrupts Scheduling and Payroll for Thousands of Employers

Logging hours manually may be only recourse

December 15, 2021

A ransomware attack on a major HR technology provider is creating chaos around attendance, scheduling and payroll for thousands of employers—with no certain end to the problem in sight.

Ultimate Kronos Group (UKG) revealed that one of its cloud-based time and attendance systems—Kronos Private Cloud—was exploited by hackers and that the outage could last several weeks. That's especially distressing news due to the increased use of variable staffing and vacation scheduling during the holidays and the calculation of end-of-year payroll concerns such as bonuses.

Kronos Private Cloud includes the products UKG Workforce Central, UKG TeleStaff, Healthcare Extensions and Banking Scheduling Solutions.

"It could not be worse timing, as many companies employing hourly workers are busier during the holiday season and having to track more overtime," said Sam Grinter, senior principal analyst at advisory firm Gartner, based in London. "The attack not only comes during the crucial end of the year for scheduling and staffing but also right when UKG's annual customer conference was getting underway."

The attack, discovered Dec. 11, has affected 2,000 organizations that use the software, including enterprise companies, hospitals, government agencies, universities, and emergency services like fire and police departments.

"Clients are very worried about this and are trying to figure out what to do," Grinter said. "It's not something we've seen before on this scale, on the HR side."

UKG said all products linked to the Kronos Private Cloud are unavailable, and it could take up to several weeks before service is restored.

"We are working with leading cyber security experts to assess and resolve the situation, and have notified the authorities," UKG executive vice president Bob Hughes said in a statement. "The investigation remains ongoing, as we work to determine the nature and scope of the incident."

There is no reported impact to the affected products if they were installed on-premises (not pulled in from servers in the cloud), nor other UKG products such as UKG Pro, UKG Ready and UKG Dimensions, which are housed in separate environments and not in the Kronos Private Cloud.

Grinter explained that ADP could be another vendor to watch, as it resells UKG Workforce Central as an ADP product. In addition, most major payroll providers have integrations with UKG (due to the 2020 merger (www.shrm.org/resourcesandtools/hr-topics/technology/pages/kronos-ultimate-software-merger-mean-for-hr.aspx) with time and attendance pioneer Kronos).

UKG has been providing daily updates on the emergency (https://www.ukg.com/KPCupdates), including informing clients that backup systems were unavailable due to the attack; that the company had not discovered that the hackers stole any data; and that "in most instances, UKG timeclocks will record and store employee punches offline until connectivity can be restored. ... However, UKG strongly recommends customers consider manual time collection efforts to ensure accurate collection of employee time in the interim."

Feedback

Amber Clayton, director of the HR Knowledge Center at the Society for Human Resource Management, told *USA Today* (https://www.usatoday.com/story/tech/2021/12/14/kronos-ransomware-attack-payrolls/6505923001/) that most companies will be tracking timesheets or pay by hand. "Some employers may require workers to do that or ask them to write down their own hours," she said. "If not, it's always a good idea to still go ahead and do that for yourself so that you know what you've worked and how many overtime hours—things of that nature. Then that way, you can compare it to what the employer has and make sure that you're paid appropriately."

Grinter said most UKG customers commenting on the company's blog have said they will use Word or Excel to track attendance and hours. "But there are obvious problems with that," he added. "It is hard to authenticate and audit, and more intensive to administer."

He said another option is to just pay everyone the same as the previous pay cycle and try to figure out a way to straighten it out later. The problems with that approach include not being able to factor in those who worked more hours or fewer hours, not being able to pay new hires, and sending out checks to people who have left the organization, Grinter said.

"Some clients are shopping around for new solutions, but the problem there is that will take weeks or months to accomplish," he said. "That is not a short-term solution, except maybe for those customers who may be using UKG for time and attendance but are also using Oracle or Workday or another big vendor for HCM. Because they are already a client of those vendors and those vendors have time management as part of their suite, it would take less time to transfer over, but it still isn't a very quick solution."

Feedback

As for alleviating the situation by paying the ransom, UKG's actions so far indicate it is not going to take that route, but that could change, Grinter said.

Allan Liska, an intelligence analyst at Somerville, Mass.-based cybersecurity firm Recorded Future, said that even if the company decides to pay the ransom, it can take days to negotiate a settlement and put together the funds. And malware could be left behind for future ransom demands or other exploits. The only safe course is a complete rebuild of the server network, he said.

Protecting Employee Data

UKG has not determined whether the incident has impacted customer data. But the extent of employee information stored in Kronos Private Cloud—and therefore potentially exposed—varies by employer. The city of Cleveland for example, warned its workforce that names, addresses and the last four digits of Social Security numbers could be at risk.

"UKG has been notifying affected customers, and those customers are obviously working with UKG to ascertain what data was included and whether that data was exfiltrated prior to the deployment of the ransomware," said Linn Freedman, a partner in the Providence, R.I., office of law firm Robinson & Cole. "Companies can proactively determine what may have been compromised by doing their own analyses. Companies will have to determine what data was compromised, what their legal obligations are and what their contractual agreements are with UKG for that process."

Stephen Cavey, co-founder of Ground Labs, a cybersecurity firm in Singapore, said that while it is too late to avoid the breach and secure exposed data, employers should seek to invest in scanning and remediation technology as soon as possible.

"These technologies help businesses understand not only where data resides, but also the type, sensitivity and amount that needs to be protected," he said. "Scanning and remediation technology also can help impacted businesses in similar situations to UKG strategically remediate vulnerabilities and protect consumers and their privacy so that future scenarios like this one do not repeat."

Is Log4j the Culprit?

It is being theorized that the UKG ransomware attack may be related to the recently disclosed Log4j vulnerability. The bug, also known as Log4Shell, was discovered in a commonly used bit of Java software on Dec. 9.

Officials at the U.S. Cybersecurity and Infrastructure Security Agency have since warned that state-sponsored hackers from China, Iran and North Korea have started testing and exploiting the vulnerability, which allows remote attackers to take over a device. The agency said hundreds of millions of enterprise and consumer devices are at risk until the bug is patched.

Tech companies have been scrambling to address the threat, but organizations and consumers should immediately patch any applications or systems affected by it, if possible, according to cybersecurity experts.

UKG maintains that there is no connection to Log4j. "We are investigating whether or not there is any relationship between the security incident and the Log4j vulnerability," UKG said.

"The vulnerability's appearance is at the very least coincidental," Freedman said. "Time will tell whether it is related to the attack, but the Log4j vulnerability is concerning. The ultimate effect of it will be very significant."

Preparing for Ransomware Attacks

Freedman said the ransomware attacks we're seeing are just the beginning of a disturbing trend. "There has been an increase in the number of cyberattacks against companies that have access to many other companies' data," she said, citing the data breach at file-sharing firm Accellion in December 2020 and numerous attacks against managed IT service providers this year. "These criminals want to inflict as much pain as possible," she said.

"The big lesson is that companies must have specific contingent operations and backup plans in place for when a critical third-party service provider is taken out," Freedman continued. "This will not be the last time this will happen."

She said there's a long list of things companies can and should do to mitigate the effects of a ransomware attack, but they should also know that these events cannot be completely prevented.

Those action items include the development of contingent and backup plans, disaster recovery plans, remote desktop protocol monitoring, insider threat intelligence, multifactor authentication on all applications and strong spam filters. "Even all of the most effective security measures, however, can never completely prevent a cyberattack," she said.

Feedback

HR DAILY NEWSLETTER

News, trends and analysis, as well as breaking news alerts, to help HR professionals do their jobs better each business day.

CONTACT US (WWW.SHRM.ORG/ABOUT-SHRM/PAGES/CONTACT-US.ASPX) | 800.283.SHRM (7476)

© 2021 SHRM. All Rights Reserved

SHRM provides content as a service to its readers and members. It does not offer legal advice, and cannot guarantee the accuracy or suitability of its content for a particular purpose.

Disclaimer (www.shrm.org/about-shrm/Pages/Terms-of-Use.aspx#Disclaimer)

Feedback