CDK Global cyberattack impacts thousands of US car dealerships

By **Lawrence Abrams**

June 19, 2024 01:58 PM 0

Further updates added to the bottom of the article.

Car dealership software-as-a-service provider CDK Global was hit by a massive cyberattack, causing the company to shut down its systems and leaving clients unable to operate their business normally.

CDK Global provides clients in the auto industry a SaaS platform that handles all aspects of a car dealership's operation, including CRM, financing, payroll, support and service, inventory, and back office operations.

The company is used by over 15,000 car dealerships in North America and has thousands of employees throughout the country.

To use CDK's services, car dealerships configure an always-on VPN to the SaaS provider's data centers, allowing their locally installed applications to access the platform.

Last night and into this morning, CDK Global suffered a cyberattack that caused it to shut down its IT systems, phones, and applications to prevent the attack's spread.

Brad Holton, CEO of Proton Dealership IT, a cybersecurity and IT services firm for car dealerships, told BleepingComputer that the attack caused CDK to take its two data centers offline at approximately 2 AM last night.

Employees at multiple car dealerships have also told BleepingComputer that CDK has not shared much information other than to send an email warning that they suffered a cyber incident.

"We are currently experiencing a cyber incident. Out of caution and concern for our customers, we have shut down a majority of our systems," reads an email shared with BleepingComputer.

"We are currently assessing the overall impact and currently have no ETA."

Some of these employees have also shared concerns that threat actors could use the always-on VPN to pivot into the internal network of car dealerships.

An IT professional for one dealership told BleepingComputer CDK advised them to disconnect the always-on VPN out of caution.

Holton explained that CDK software running on devices has administrative privileges used to deploy updates, which could explain why CDK recommends disconnecting from the data centers.

While some users have stated that they can log in with old credentials that were upgraded during CDK's transition to a modern single-sign-on platform, BleepingComputer has been told that the application does not work as expected.

> If you have any information regarding this incident or any other undisclosed attacks, you can contact us confidentially via Signal at 646-961-3731 or at tips@bleepingcomputer.com.

Widespread disruption

The outage has led to widespread disruption among car dealerships using their platform to track and order car parts, conduct new sales, and offer financing.

Employees have reported on Reddit that they were left with nothing to do or were forced to go back to paper and pencil. Some dealerships are sending employees home for the day due to the outages.

"We are almost to that point... no parts, no ROs, no times... just dead vehicles with nothing to show for them or parts to fix them," a dealership employee posted to Reddit.

"Excel spreadsheets and post it notes for any parts we're handing out. Any big jobs are not happening," another employee commented.

While there has been no official statement from CDK, it is rumored that the company suffered a ransomware attack that also impacted its backups.

BleepingComputer has been unable to confirm this information independently, but if it was a ransomware attack, the outages will likely last for days, if not into next week and longer.

When ransomware gangs breach corporate networks, they quietly spread to other devices while stealing corporate data.

Once all data has been stolen and the threat actors gain administrative privileges, they encrypt all of the devices on the network, leaving behind ransom notes with instructions on contacting the hackers.

The encrypted devices and stolen data are used in double-extortion schemes, where the threat actors demand a ransom payment to provide a decryptor and to delete and not publish any stolen data.

These negotiations can take weeks, and if a ransom is not paid, the threat actors ultimately leak the corporate data, which usually includes the personal information of employees and, potentially, customers.

Update 6/19/24: CDK shared the following statement with BleepingComputer:

> "We are actively investigating a cyber incident. Out of an abundance of caution and concern for our customers, we have shut down most of our systems and are working diligently to get everything up and running as quickly as possible." - CDK.

Update 6/19/24 5:24 PM ET: CDK has shared an update with customers stating that they have restored CDK Phones, DMS and Digital Retail. They have also stated that Unify and DMS logins are now available.

However, they are continuing to conduct tests on all other applications before bringing them back online.

BREACH | CAR DEALERSHIP | CDK GLOBAL | CYBERATTACK | DATA CENTER | OUTAGE

LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE | NEXT ARTICLE