# Exclusive: Apex Custom Software hacked, threat actors threaten to leak the software (1) - DataBreaches.Net

Published: 2025-01-30 · Archived: 2026-04-11 02:13:35 UTC

On January 20, the hackers known as 0mid16B tweeted, “At 7:40AM 20th Jan (US time), a US healthcare software provider has been hacked. All data in server has been deleted. 48 hours left before we publish all data.” The attached screenshot showed a listing of medications, but without any patient information attached. Two days later, they tweeted information about Cardinal Health, but again, it did not appear linked to any protected health information (PHI). They also published some Cardinal Health employee login information that included names, email addresses, and passwords in plaintext.

Cardinal Health isn’t a software provider. And as the hackers revealed in a January 26 tweet, it was **Apex Custom Software (“Apex”)** in Texas that they had hacked. Cardinal was only one of its clients who were allegedly affected.

Apex specializes in software for the healthcare sector. Its products focus on controlled substance tracking, credentialing management, inventory management, telemedicine, and healthcare analytics.

On January 26, 0mid16B reached out to DataBreaches.net and provided additional information about the attack, accompanied by what they described as the entire databases of Apex’s software.

## What Happened?

In response to specific questions posed by DataBreaches, the spokeserson for 0mid16B stated that they first accessed Apex between January 16 – January 20. They declined to reveal how they gained access, but claim that Apex never detected their presence or the exfiltration. As of January 29, they claimed they still had access.

0mid16B states they first contacted Apex on January 20. “They responded, but the owner said he has no money and only offered 1000 USD,” 0mid16B told DataBreaches.

Although they tweeted about Cardinal Health, 0mid16B stated that they did not contact Cardinal Health or any other client directly. They were “Pissed at APEX offer and decided to publish all.” The spokesperson later added, “In fact, i told him that we know he owns 1 million USD bungalow and a 400,000 USD apartment when he told us he is poor and can only pay 1000 USD.” DataBreaches does not know if that is true, but has seen this type of thing a number of times where threat actors have researched their victims carefully and know when victims are lying about their revenue or assets. Maybe the owner expected 0mid16B to respond with another, and lower, demand than their original demand. If so, he miscalculated.

DataBreaches asked 0mid16B what they had meant in earlier correspondence about the importance of auditing software for security before contracting with a software provider. DataBreaches asked, “You said auditing software companies is important. What would an audit of Apex have shown Cardinal?” 0mid16B responded, “Their security is none. It is standard operating procedure to audit coding before going LIVE. An audit of APEX

software would tell the world, never to engage their services. APEX designed loopholed softwares and used unsecured backend for storing data and they are focused on healthcare software?"

If 0mid16B does wind up leaking all the software, others will be able to conduct an audit to confirm or refute their claims about APEX's lack of security.

## Risk to Patients?

One of DataBreaches' other questions concerned how much protected health information (PHI) there was in the data, as looking through the software data provided to this site, DataBreaches did not see a lot of PHI. But there are also other risks possibly involved, apart from the firm having its propietary information leaked publicly. DataBreaches asked 0mid16B about what a malicious threat actor could do with access.

"Theoretically, we can make a change to scheduled dispensing, say Drug A and change it to Drug B and the drug will be dispensed wrongly to the end user," they answered. "Of course, we wouldn't be doing this but that is already dangerous, even without PHI." DataBreaches notes that healthcare professionals routinely verify that they are administering the correct medication and dosage to patients, but if someone tampered with inventory so that hospitals or pharmacies ran out of medications they needed for patient care, that could impact patient care. But to be clear: there is no indication that 0mid16B has any intention of doing anything malicious. They are a financially motivated group who has been increasingly turning to the U.S. healthcare sector because, as 0mid16B told DataBreaches in an earlier communication, unlike India and Canada, U.S. healthcare victims pay.

## How Has Apex Responded?

DataBreaches reached out to to Apex via email on January 27 and again on January 29. The second email informed Apex of some of 0mid16B's claims and asked what they were doing in response. No reply has been received.

DataBreaches also reached out to Cardinal Health via email yesterday to ask whether Apex had notified them of them the incident. They, too, did not reply, and DataBreaches does not know if they are even aware that some employee login credentials have been leaked publicly in plain text.

Today, HHS's update included an entry for Apex Custom Software that was submitted to them on January 22. The report, submitted as a business associate, indicated that 1,500 patients had been affected. It is not clear if that number is on behalf of all of its clients or just one or a few. There is no notice on Apex's website about any incident.

As of publication, 0mid16B does not appear to have leaked the software on the forum where they usually leak data.

**Update of February 1.** 0mid16B leaked the Apex Controlled Substance software and also leaked what appears to be some employee information from Cardinal Health that includes passwords in plain text.

---