

**UNITED STATES
SECURITIES AND EXCHANGE COMMISSION**
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 OR 15(d) of The Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): **August 24, 2026**

NUTEX HEALTH INC.
(Exact name of registrant as specified in its charter)

Delaware	001-41346	11-3363609
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

1776 Yorktown Street, Suite 700, Houston, Texas 77056
(Address of principal executive offices) (zip code)

(713) 660-0557
(Registrant's telephone number, including area code)

N/A
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- ☐ Written communication pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- ☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- ☐ Pre-commencement communication pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- ☐ Pre-commencement communication pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock, \$0.001 par value	NUTX	The NASDAQ Stock Market LLC

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR §230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR §240.12b-2).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 8.01 Other Events.

Nutex Health Inc. (the "Company") recently learned of unauthorized activity involving data stored on its computer network. As a result, the Company has engaged an independent third-party cybersecurity response team and forensic experts, activated a cybersecurity response plan, implemented containment measures and notified law enforcement.

Based on preliminary findings from the Company's ongoing investigation, the Company believes that certain information maintained on the Company's servers was accessed and exfiltrated by an unauthorized third party, including some information that may be private and/or confidential. To date, the Company has not identified any material impact on its business operations or financial reporting systems.

The Company continues to assess whether, and to what extent, patient, employee, credentialed provider, confidential business and financial information, intellectual property, or other information may have been accessed, acquired, or exfiltrated and continues to evaluate the potential impact of the unauthorized activity on the Company, including any potential disclosure of private and/or confidential information by the third party.

As of the date of this Current Report on Form 8-K, the Company does not believe that the unauthorized access has had, or is reasonably likely to have, a material impact on the Company's business strategy, operations, financial condition or results of operations.

The Company continues to evaluate applicable regulatory and legal notification requirements, and the Company intends to make all required notifications based on its findings, including to impacted patients, if applicable.

Forward-Looking Statements

This Current Report on Form 8-K contains "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. Such forward-looking statements are intended to be covered by the safe harbor provisions for forward-looking statements contained in the Private Securities Litigation Reform Act of 1995 and are included in this statement for purposes of complying with these safe harbor provisions. This document contains certain forward-looking statements with respect to current beliefs, understanding and expectations regarding the incident and its remediation and investigation. These forward-looking statements can be identified by the fact that they do not relate only to historical or current facts. Forward-looking statements often use words such as "estimate," "project," "predict," "will," "would," "should," "could," "may," "might," "anticipate," "plan," "intend," "believe," "expect," "aim," "goal," "target," "objective," "commit," "advance," "likely" or similar expressions that convey the prospective nature of events or outcomes.

These forward-looking statements reflect current beliefs, understanding and expectations regarding the incident and its remediation and investigation. Factors that could cause actual results to differ materially from those indicated in the forward-looking statements include, but are not limited to: the results of the Company's ongoing investigation and analysis of the scope and details of the cybersecurity incidents and the potential discovery of new and additional information related thereto; the Company's expectations regarding its ability to contain and remediate the cybersecurity incidents, including the success of containment and remediation activities to date; any unauthorized release of the Company's data, including third-party data held by the Company, or the use of any such data for fraudulent purposes; potential loss or destruction of Company data or adverse impacts to the Company's operations; the impact of the cybersecurity incidents on the Company's relationships with customers, employees, governmental regulators, and other stakeholders; diversion of management's attention from the Company's operations to addressing the cybersecurity incidents; the legal, reputational, and financial risks resulting from the cybersecurity incidents, including those that may arise from any potential regulatory inquiries and/or litigation to which the Company may become subject in connection with the incidents; other reputational risk related to the cybersecurity incidents; regulatory scrutiny of the cybersecurity incidents; risks related to the availability of the Company's insurance coverage for losses and costs associated with the cybersecurity incidents; and remediation and other additional costs that may be incurred by the Company in connection with the investigation and remediation of the incidents. Readers are cautioned that these forward-looking statements are not guarantees of future events or outcomes and they should not be unduly relied on, as they are based on information available to the Company and on management's current beliefs and expectations as of the date of this Current Report on Form 8-K and are therefore inherently uncertain and subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in our filings with the Securities and Exchange Commission, including the risk factors contained in our most recent Annual Report on Form 10-K and our Quarterly reports on Form 10-Q for the periods ended March 31, 2026 and June 30, 2026. We undertake no obligation to revise or update any forward-looking statements, including to reflect events or circumstances occurring after the date of the filing of this report, except to the extent required by law.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned, hereunto duly authorized.

Date: August 24, 2026

NUTEX HEALTH INC.

By: */s/ Jon C. Bates*

Jon C. Bates

Chief Financial Officer