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) January 17, 2024

Microsoft Corporation

Washington	**001-37845**	**91-1144442**
(State or Other Jurisdiction of Incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

One Microsoft Way, Redmond, Washington	**98052-6399**

(425) 882-8080
www.microsoft.com/investor

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 (see General Instruction A.2. below):

☐ Written communications 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 communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications 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	Name of exchange on which registered
Common stock, $0.00000625 par value per share	MSFT	NASDAQ
3.125% Notes due 2028	MSFT	NASDAQ
2.625% Notes due 2033	MSFT	NASDAQ

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter). 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 1.05. Material Cybersecurity Incidents

On January 12, 2024, Microsoft (the "Company" or "we") detected that beginning in late November 2023, a nation-state associated threat actor had gained access to and exfiltrated information from a very small percentage of employee email accounts including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, on the basis of preliminary analysis. We were able to remove the threat actor's access to the email accounts on or about January 13, 2024. We are examining the information accessed to determine the impact of the incident. We also continue to investigate the extent of the incident. We have notified and are working with law enforcement. We are also notifying relevant regulatory authorities with respect to unauthorized access to personal information. As of the date of this filing, the incident has not had a material impact on the Company's operations. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

This Form 8-K contains forward-looking statements, which are any predictions, projections or other statements about future events based on current expectations and assumptions that are subject to risks and uncertainties, which are described in our filings with the Securities and Exchange Commission. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and the Company undertakes no duty to update any forward-looking statement to conform the statement to actual results or changes in the Company's expectations.

Item 7.01. Regulation FD Disclosure

On January 19, 2024, the Company posted a blog regarding the incident. A copy of the blog is furnished as Exhibit 99.1 to this report.

In accordance with General Instruction B.2 of Form 8-K, the information in this Item 7.01 and Exhibit 99.1, shall not be deemed to be "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or otherwise subject to the liability of that section, and shall not be incorporated by reference into any registration statement or other document filed under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

Item 9.01. Financial Statements and Exhibits

(d) Exhibits:

99.1	Microsoft Blog Post dated January 19, 2024 titled "Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard"
104	Cover Page Interactive Data File (embedded within the Inline XBRL document)

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.

MICROSOFT CORPORATION
(Registrant)

Date: January 19, 2024

/s/ Keith R. Dolliver
Keith R. Dolliver
Corporate Secretary

Exhibit 99.1

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

This attack does highlight the continued risk posed to all organizations from well-resourced nation-state threat actors like Midnight Blizzard.

As we said late last year when we announced Secure Future Initiative (SFI), given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient. For Microsoft, this incident has highlighted the urgent need to move even faster. We will act immediately to apply our current security standards to Microsoft-owned legacy systems and internal business processes, even when these changes might cause disruption to existing business processes.

This will likely cause some level of disruption while we adapt to this new reality, but this is a necessary step, and only the first of several we will be taking to embrace this philosophy.

We are continuing our investigation and will take additional actions based on the outcomes of this investigation and will continue working with law enforcement and appropriate regulators. We are deeply committed to sharing more information and our learnings, so that the community can benefit from both our experience and observations about the threat actor. We will provide additional details as appropriate.