Food giant WK Kellogg discloses data breach linked to Clop ransomware

By Bill Toulas

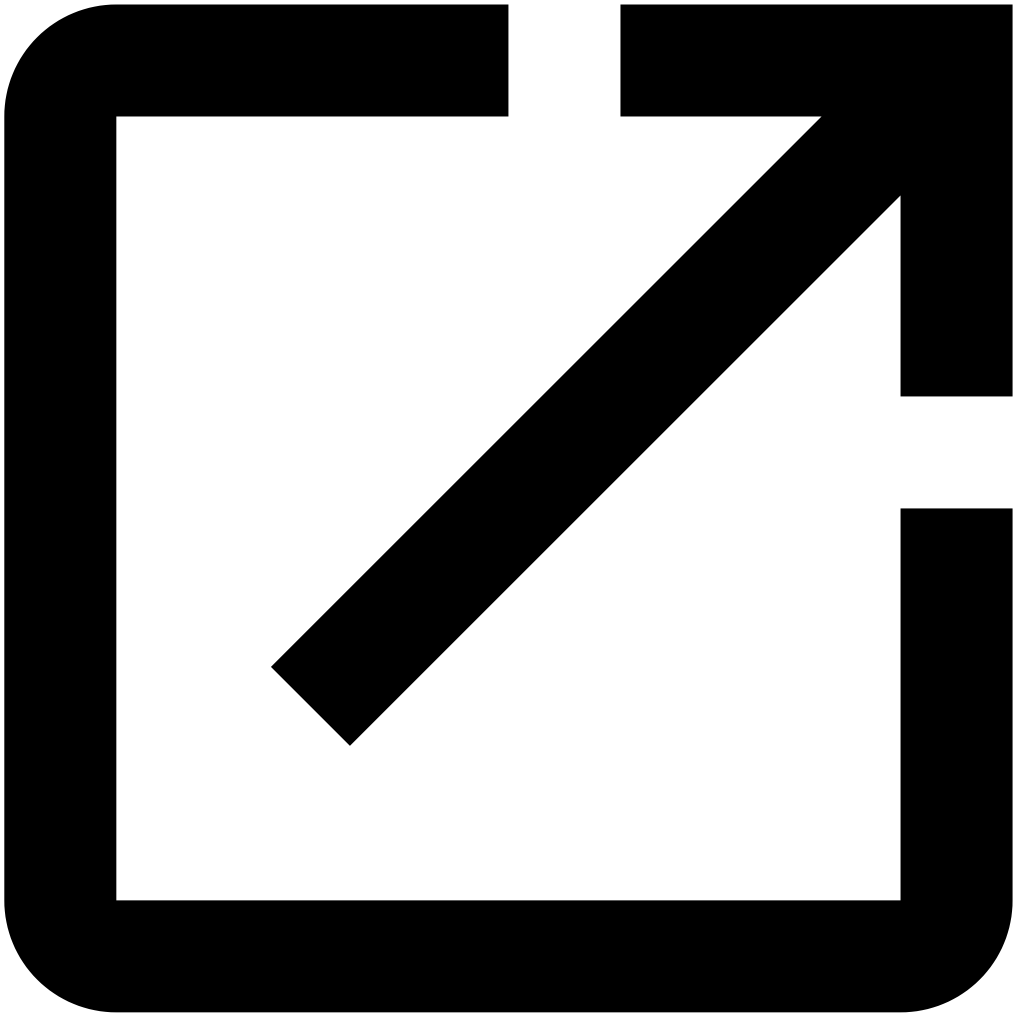
Published: 2025-04-07 · Archived: 2026-04-05 14:45:21 UTC

US food giant WK Kellogg Co is warning employees and vendors that company data was stolen during the 2024 Cleo data theft attacks.

Cleo software is a managed file transfer utility that was targeted by the Clop ransomware gang en masse at the end of last year. This attack leveraged two zero-day flaws tracked as CVE-2024-50623 and CVE-2024-55956, allowing the threat actors to breach servers and steal data.

"WK Kellogg learned on February 27, 2025, that a security incident may have occurred involving Cleo," reads the notice.


DIE LINKE.
0:00



"WK Kellogg immediately began to investigate. We contacted Cleo, and Cleo informed us that an unauthorized person gained access on December 7, 2024, to the servers Cleo hosted for us that were used for transferring employee files to our human resources service vendors."

WK Kellogg Co is an American food manufacturing giant split from Kellogg's in October 2023. It has an annual revenue of $2.7 billion and owns popular cereal brands such as All-Bran, Corn Flakes, Froot Loops, and Frosted Flakes.

Although the company does not specifically mention Clop or the data theft attacks, the date of the reported incidents coincides with the wave of attacks that occurred in December 2024.

Furthermore, the breach notifications come soon after the Clop ransomware gang listed WK Kellogg on their data leak extortion site.

The data breach notification shared with the authorities says the exposed data includes a person's name and social security number.

The letter encloses instructions on how recipients can enroll in a free one-year identity monitoring and fraud protection services through Kroll. Impacted individuals are also recommended to consider placing fraud alerts or a security freeze on their credit file.

Kellogg says it worked closely with Cleo to identify the security measures it implemented to address last year's breach and prevent similar incidents from occurring in the future.

Kellogg is the latest victim of a long list of companies impacted by Clop's Cleo zero-day attacks, with the threat actors gradually disclosing additional victims and stolen data samples several months after the incident.

The previous disclosure came on March 18 by Arizona-based Western Alliance Bank, which informed 22,000 customers their personal data had been stolen in an October 2024 breach of Cleo's secure file transfer software.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
