



Nucor



Discovered: Identified c. 13 May 2025

Sector: Manufacturing: steel

Systems Reached: Certain IT systems

Scale: "Various locations";
number of sites **undisclosed**

Initial Access Vector: Undisclosed

Attacker: Undisclosed ("a threat actor")

Root Cause: Undisclosed

Malware: Undisclosed

Operational Impact:

Production halted "in an abundance of caution"; restored by 20 June 2025; "limited data" exfiltrated

Financial Impact: Undisclosed;

Nucor: not material (8-K/A); data suit settled 2026

Process Impact: None disclosed.

No filing describes any effect on a furnace, caster, mill or control system.

Cross Reference:

Bridgestone · Ingersoll Rand · German Steel Mill

In May 2025 an intruder in Nucor's IT systems led North America's largest steel producer to halt production at various locations as a precaution. Nucor filed it as not material. No vector, actor or incident cost is on the record.

Nothing in Nucor's record says a furnace, a caster or a control system was reached. Both filings describe information technology, and production halted at various locations anyway. Nucor acted well: it filed the day after its date of report, before it knew the scale, stopped its own lines rather than wait, restored from backups, and came back five weeks later to disclose that data had left.

The finding is not that it stopped. It is that stopping was the defensible answer. When the only move an operator can prove safe is to halt the mills, the plant was already riding on the business network. That is BlastWave's analysis, not a disclosed fact. The correction is ours: our first volume gave this incident ransomware, a loss range, a downtime figure and a likely vector. None of it is in either filing.

What is not known: Nucor has not said how the intruder got in, who it was, what tooling it used, which facilities stopped or for how long. Its amendment sets limited access to IT applications supporting some operations beside a production halt made in an abundance of caution, without saying which stopped which line. No filing names ransomware or any malware. Nucor told the SEC the incident was not material and filed no cost; class action papers describe the stolen data as personal information of about 3,000 people. Whether any plant could have run without those systems is not on the record.

Recommendation

1. Take the path away

Scheduling, recipes and order release the mill needs belong on the plant side of a boundary, so containing IT is a decision about IT, not a decision to stop steel.

2. Remove standing credential access

Every remote and vendor path into plant networks is tied to a named person, scoped and revocable in one move, so containment is a policy change, not a shutdown.

3. Make the business side read one way

The office sees the mill without being able to reach back into it, and the plant keeps a rehearsed way to run a shift while the office is dark.



The Fireworks Hold

Embedded audio/file-013.m4a



Nucor Short

External Link – Opens in Browser

Sources: Form 8-K, Item 1.05, 14 May 2025 • Form 8-K/A, Item 1.05, 20 Jun 2025 • EDGAR full-text search, CIK 0000073309, 24 Sep 2026 • Sweat v. Nucor, W.D.N.C. 3:25-cv-00478, settlement approved 18 Aug 2026.

Soft Spots: That a precautionary halt shows the plants depended on business systems, or that nobody could prove they did not, is BlastWave's analysis. "Not material" is Nucor's judgement, not a statement of zero cost.