Kyocera AVX says ransomware attack impacted 39,000 individuals

By Bill Toulas

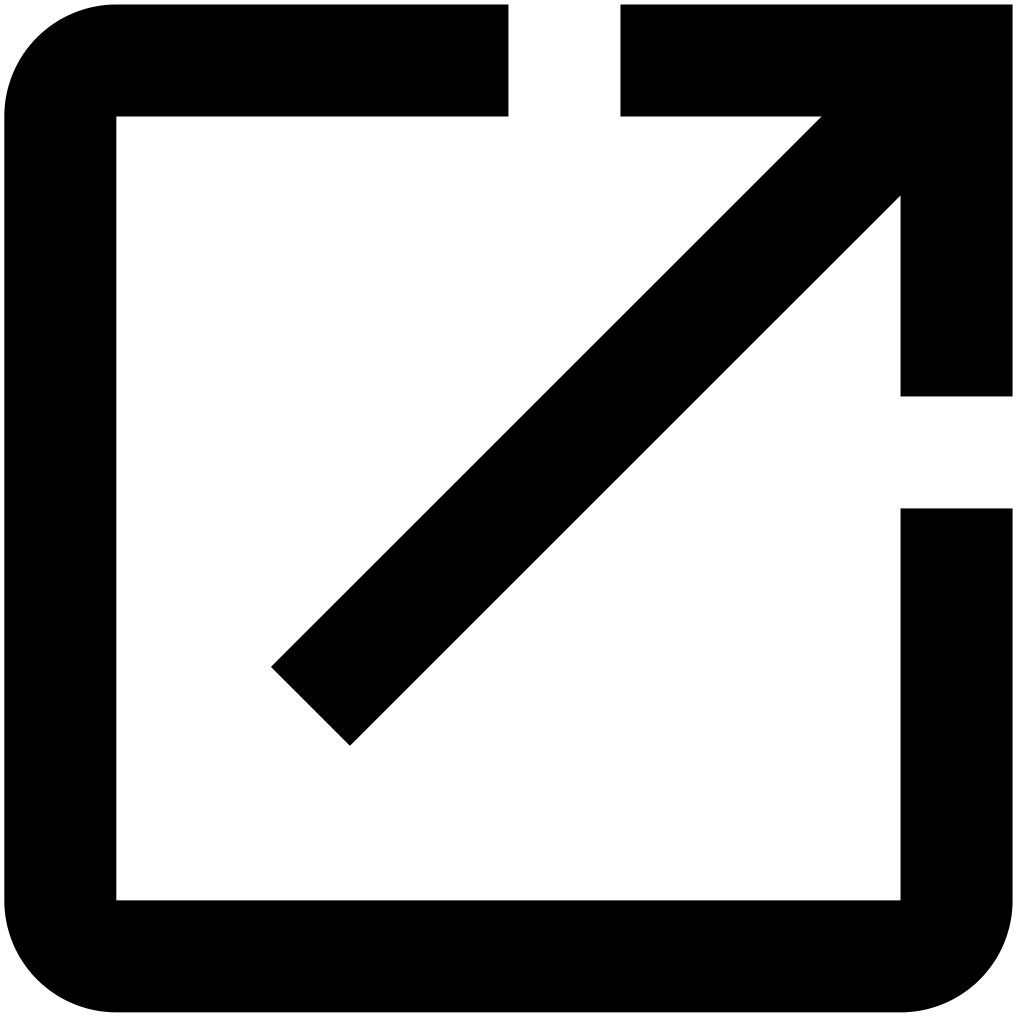
Published: 2023-11-09 · Archived: 2026-04-05 15:06:12 UTC

Kyocera AVX Components Corporation (KAVX) is sending notices of a data breach exposing personal information of 39,111 individuals following a ransomware attack.

KAVX is an American manufacturer of advanced electronic components, a subsidiary of the Japanese semiconductor giant Kyocera. It employs over ten thousand specialists and has an annual revenue of $1.3 billion.

In the data breach notification to affected people, KAVX says that it discovered on October 10, 2023 that hackers accessed its systems between February16, and March 30, 2023.


DIE LINKE.
0:00



“On March 30, 2023, KAVX experienced a cybersecurity incident affecting servers located in Greenville and Myrtle Beach, South Carolina, USA, which resulted in the encryption of a limited number of systems and temporary disruption of certain services,” reads the notice.

“KAVX later discovered that the data contained on the impacted servers included personal information of individuals globally,” the company notes.

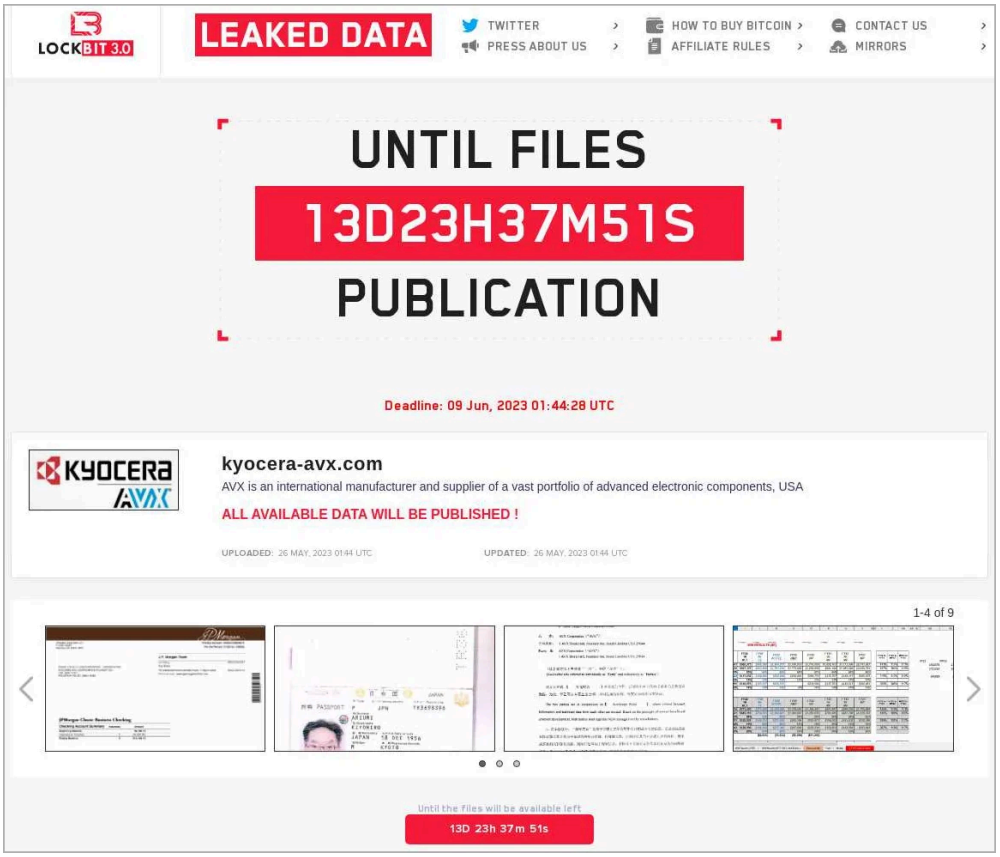
Following an internal investigation to determine what information was exposed, KAVX confirms that it includes at least full names and Social Security Numbers (SSNs). Possibly, more details were exposed, but the relevant section on the notice sample is censored.

KAVX says it has no evidence that the cyber-criminals abused the stolen data but reminds the letter recipients of the associated risk of identity theft and fraud, urging them to be cautious.

In response to the situation, the company will also cover the costs for a 12-month dark web monitoring and password leak service for all impacted individuals.

LockBit claimed responsibility

The LockBit ransomware gang claimed to have compromised KAVX on May 26, 2023, when it added the firm to its data leak site.



KAVX on the LockBit extortion portal (KELA)

The threat actors published several samples of the stolen data on their extortion portal, including passport scans, financial documents, non-disclosure agreements, and more. The deadline that the hackers had set for KAVX to pay the ransom was June 9, 2023.

Notably, LockBit also leaked component schematics and technical drawings, meaning that the incident has the potential to expose proprietary designs and patented information to competitors.

Source: https://www.bleepingcomputer.com/news/security/kyocera-avx-says-ransomware-attack-impacted-39-000-individuals/