

Public Disclosure of Cyber Incident

Third Party Vendor MOVEit Breach: Maximus

Along with numerous public and private entities throughout the United States, the State of Maryland was impacted by a vulnerability (CVE-2023-34362) in a file transfer application, MOVEit. On May 30, 2023, a malicious actor exploited the MOVEit vulnerability CVE-2023-34362 via a third party vendor, Maximus, used by the State of Maryland's Department of Human Services. Maximus aggregates new hire data submitted by for-profit and nonprofit Maryland businesses and State agencies.

The actor was able to gain access to a Maximus MOVEit file transfer server that processed Personally Identifiable Information (PII) for residents and businesses within the State. Maximus identified the malicious activity within 24 hours, remediated it, and engaged with external forensics and data investigators to identify the scope of the compromise.

As a result of its investigation, Maximus identified that approximately 0.3% of the Maryland records processed by it were retrieved or viewed by the actor. The records of approximately 5,000 individuals and 200 businesses were compromised. Information breached by the actor includes a combination of:

1. Full Social Security Numbers (SSN)
2. Employer Identification Numbers (EIN)
3. Home Addresses
4. Dates of Birth

Maximus is sending breach notification letters to impacted parties at the same time as this public release. While the investigation found no known misuse of the PII, Maximus is offering credit monitoring services available free of charge to impacted parties. A call center specific to this event has been set up by Maximus for 90 days to support enrollment into the credit monitoring service and answer any questions individuals may have. The call center is reachable by toll-free number at 833-919-4749 Monday through Friday between 9:00 a.m. and 11:00 p.m. Eastern Standard Time, or Saturday and Sunday between 11:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding major U.S. holidays). Additional information about the credit monitoring services will be provided in the Maximus notification letter.



Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary
Melissa Leaman | Deputy Secretary

It is recommended that all individuals generally, and as affected by this incident, closely monitor financial account statements and credit reports and report any discrepancies to law enforcement. Additional guidance that consumers can take to protect themselves is provided by the [Federal Trade Commission's Consumer Advice on Identity Theft](#).

The US Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) first posted an advisory regarding a vulnerability in the MOVEit file transfer application on the 1st of June 2023. On the 7th of June, CISA published a second advisory in which CISA advised that actors were using the vulnerability to exfiltrate data from numerous public agencies and private businesses across the country. The State of Maryland and our vendors are continuing to comply with federal investigations into specific threat actor(s) and their activity.

This public notification is given consistent with the requirements of the [Guidelines for the Public Disclosure of Cybersecurity Incidents](#) adopted by the Maryland Department of Information Technology.