Data breach exposes 1.6 million Washington unemployment claims

By Lawrence Abrams

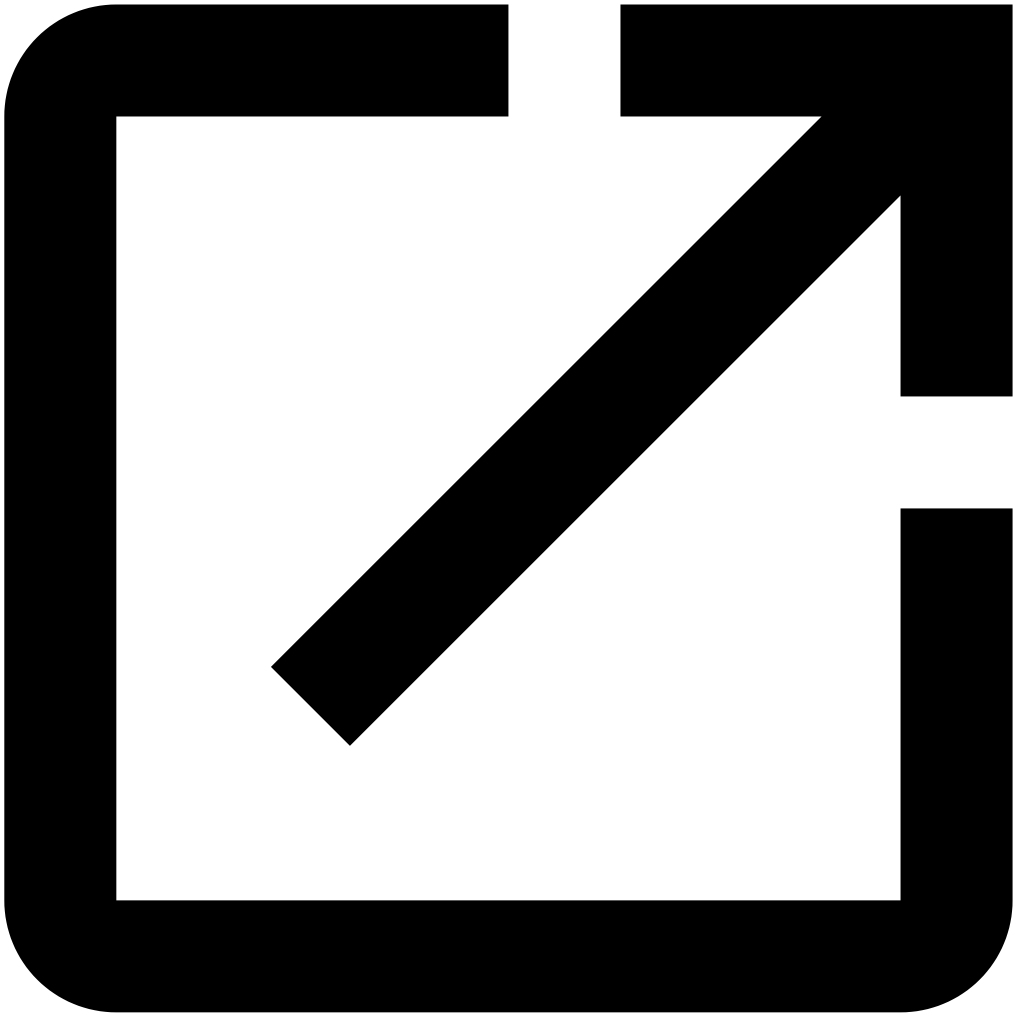
Published: 2021-02-01 · Archived: 2026-04-05 13:55:55 UTC

Washington's State Auditor office has suffered a data breach that exposed the personal information in 1.6 million employment claims.

The Office of the Washington State Auditor (“SAO”) states that they suffered a data breach after a threat actor exploited a vulnerability in a secure file transfer service from Accellion.

"SAO is advised that an unauthorized person was able to exploit a software vulnerability in Accellion’s file transfer service and gain access to files that were being transferred using Accellion’s service. Accellion stated that they believe the unauthorized access occurred in late December of 2020."


DIE LINKE.
0:00



Visit Advertiser websiteGO TO PAGE

"Other customers of this Accellion service were similarly impacted. SAO is currently seeking a full understanding of the timeline of the incident and the status of Accellion's investigation and the investigation by law enforcement. At this time, SAO does not have enough information to draw conclusions about the timing or full scope of what took place."

"It was not until the week of January 25, 2021, that Accellion confirmed to SAO that SAO files were subject to this attack and provided the information needed for SAO to begin to identify which data files were impacted and individuals whose personal information is in those files," SAO stated in a security breach notification posted to their website.

The exposed claims were in data files from the Employment Security Department (ESD) and contain sensitive personal information of Washington residents.

"These ESD data files contained unemployment compensation claim information including the person's name, social security number and/or driver's license or state identification number, bank account number and bank routing number, and place of employment," the breach notification explains.

In addition to unemployment claims, the breach exposed files from some Washington local governments and other state agencies were also affected.

The SAO is still investigating what information is contained in these files.

Zero-day responsible for December attacks

Accellion is a provider of secure file transfer services that allow organizations to securely share sensitive documents with users outside their organization. This service is popular among banks, government agencies, and financial organizations that commonly share sensitive documents with external users.

Accellion stated that they became aware of an actively exploited zero-day vulnerability in their legacy FTA solution in mid-December, and a patch was deployed to all customers.

BleepingComputer later learned from one of Accellion's customers that the modern secure file sharing service, Accellion KiteWorks, also received a security update in December 2020. Accellion has not responded to our questions regarding this update.

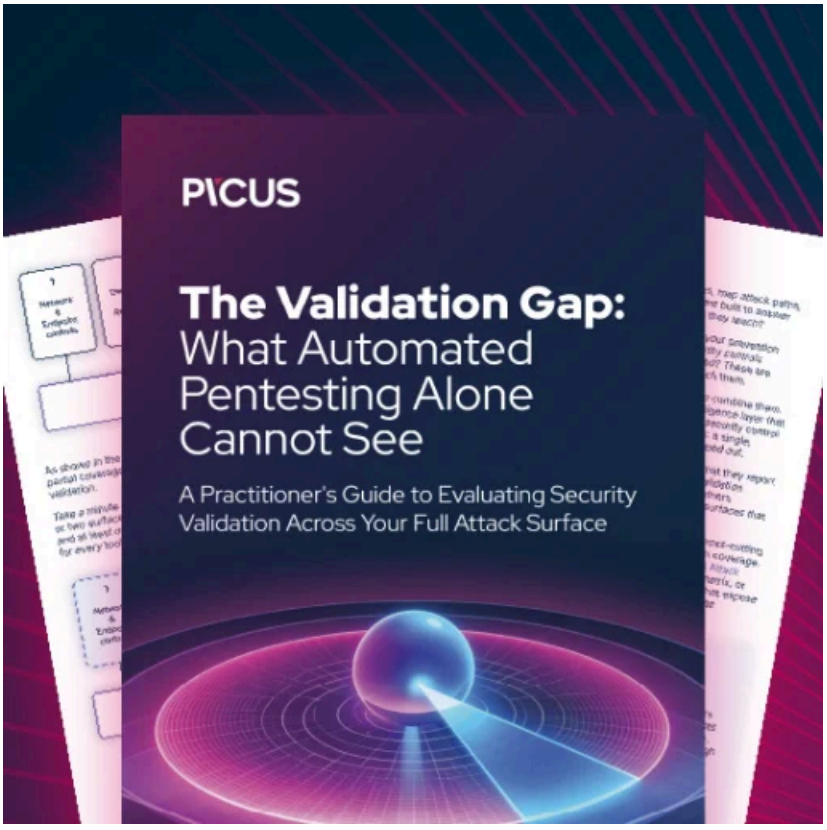
Unfortunately, numerous organizations were breached before they could deploy the patch for this vulnerability, including the Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Harvard Business School.

"In late December, Harvard Business School (HBS) was informed by one of its vendors of a vulnerability in the vendor's software. HBS applied a patch supplied by the vendor to resolve the vulnerability. On December 29, 2020, the vendor notified HBS that it had identified unauthorized access to certain HBS files."

"HBS immediately launched an investigation and determined that files containing personal information were downloaded by one or more unauthorized third parties between December 21 and December 23, 2020," the Harvard Business School told BleepingComputer in a statement.

Sources in the cybersecurity industry have told BleepingComputer that Accellion's software's vulnerability also caused the Harvard Business School breach.

With Accellion being a popular service used by numerous organizations, we should expect to see a steady trickle of similar breaches revealed soon.



Automated Pentesting Covers Only 1 of 6 Surfaces.

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.

Source: https://www.bleepingcomputer.com/news/security/data-breach-exposes-16-million-washington-unemployment-claims/