Jennifer Johnson

From: WebEOCMail-imd.idaho.gov@webeocasp.com
Sent: Tuesday, September 22, 2026 8:40 AM
Subject: Boise State University Breach Cybersecurity Reporting
Attachments: Boise State Breach.pdf

Boise State Breach Reporting 9/22/2026 8:27:15 AM

Incident

Elsevier is a Dutch academic publisher owned by RELX and one of the largest scientific publishers in the world. Beginning at 6:49pm, reports began to surface that several of the websites were redirecting to a page created by LAPSUS$, an known hacking group. Upon investigation of the Elsevier services used by Boise State, SSO to Interfolio (Faculty 180). Additional services include access to journals and coursework but do not contain sensitive data.

At 9:09pm, the redirects seem to have been removed but Boise State choose to leave SSO disabled out of caution.

At 8:30 on 9/22, after reviewing reports of the incident, the decision was made to reenable SSO. Interfolio was not impacted and there is no indication of any data was actually compromised. The attackers also did not demand any ransom.

At this juncture, the motive remains unclear. There has been no public statement by Elsevier. There is no indication that any data was ever inappropriately accessed other than redirecting the websites themselves. This did not directly impact any services hosted by Boise State.

WebEOC Log In

Cybersecurity Reporting Details

Search

Back

Incident Tracking

Remove Record

Incident ID	15
Source ID	
Incident or Breach	Incident
Incident/Breach Summary	Elsevier is a Dutch academic publisher owned by RELX and one of the largest scientific publishers in the world. Beginning at 6:49pm, reports began to surface that several of the websites were redirecting to a page created by LAPSUS$, an known hacking group. Upon investigation of the Elsevier services used by Boise State, SSO to Interfolio (Faculty 180). Additional services include access to journals and coursework but do not contain sensitive data. At 9:09pm, the redirects seem to have been removed but Boise State choose to leave SSO disabled out of caution. At 8:30 on 9/22, after reviewing reports of the incident, the decision was made to reenable SSO. Interfolio was not impacted and there is no indication of any data was actually compromised. The attackers also did not demand any ransom. At this juncture, the motive remains unclear. There has been no public statement by Elsevier. There is no indication that any data was ever inappropriately accessed other than redirecting the websites themselves. This did not directly impact any services hosted by Boise State.
Attachments	

Victim Demographics

Victim ID	512
Primary Industry	Educational Services
State	Idaho

Incident Description

Actors: External	
External: Motive	Unknown
External: Variety	Unaffiliated
Actors: Internal	
Internal: Motive	NA
Internal: Variety	
Actors: Partners	
Partner: Motive	NA
Partner: Industry	Public Administration

Actions

Actions: Malware	
Malware: Varieties	
Malware: Vector	
Malware: Common Name	
Actions: Hacking	
Hacking: Variety	URL redirector abuse
Hacking: Vector	Web application
Hacking: CVE's Exploited	Unknown
Actions: Social	
Social: Variety	Unknown
Social: Vector	Unknown
Social: Target	Unknown
Actions: Misuse	
Misuse: Variety	Unknown
Misuse: Vector	Unknown
Actions: Physical	
Physical: Variety	Unknown
Physical: Vector	Unknown
Physical: Location	Unknown
Actions: Error	
Error: Variety	Misdelivery
Error: Vector	Unknown
Actions: Environmental	
Environmental: Variety	

[Return to Beginning]

Assets

Assets: Variety	Unknown
Assets: Ownership	Partner
Assets: Management	External
Assets:Hosting	External
Assets: Accessibility	External
Assets: Cloud	Customer attack

Attributes: Availability/Utility	
Confidentiality: Disclosure	No
Confidentiality: Variety	Unknown
Confidentiality: Amount	
Confidentiality: State	Unknown
Attributes: Integrity/Authenticity	
Integrity: Variety	Unknown
Attributes: Availability/Utility	
Availability: Variety	Interruption
Availability: Duration	2Hours
Discovery & Response	
Incident Timeline: Incident Date	09/21/2026
Incident Timeline: Time to Compromise	NA
Incident Timeline: Exfiltration	NA
Incident Timeline: Discovery	NA
Incident Timeline: Containment	NA
Discovery Method	Int - reported by user
Corrective Actions	NA - Boise State uses these services but does not host them.
Targeted vs Opportunistic	NA
Impact Assessment	
Loss Categorization	No known loss of data loss or direct access to any Boise State data or systems.
Estimation Currency	Insignificant

[Return to Beginning]