CVE-2022-28924: Sensitive Information Disclosure Vulnerability in UniverSIS

By Stavros Mekesis on April 04, 2022

CVE-ID: CVE-2022-28924
Affected Products: UniverSIS-students versions prior to 1.5.0
Class: Exposure of Resource to Wrong Sphere (CWE-668)
Discovered by: Stavros Mekesis

Vulnerability Details

An Information Disclosure vulnerability exists in UniverSIS-students versions prior to 1.5.0 due to unrestricted access to some particular OData Properties through the UniverSIS API. By sending a specially crafted HTTP GET request to a vulnerable UniverSIS API endpoint such as `/api/students/me/courses/` , an authenticated student could exploit this vulnerability to obtain sensitive information (e.g. middle name, Social Security number, and home address) about all instructors in his or her department.

Proof of Concept

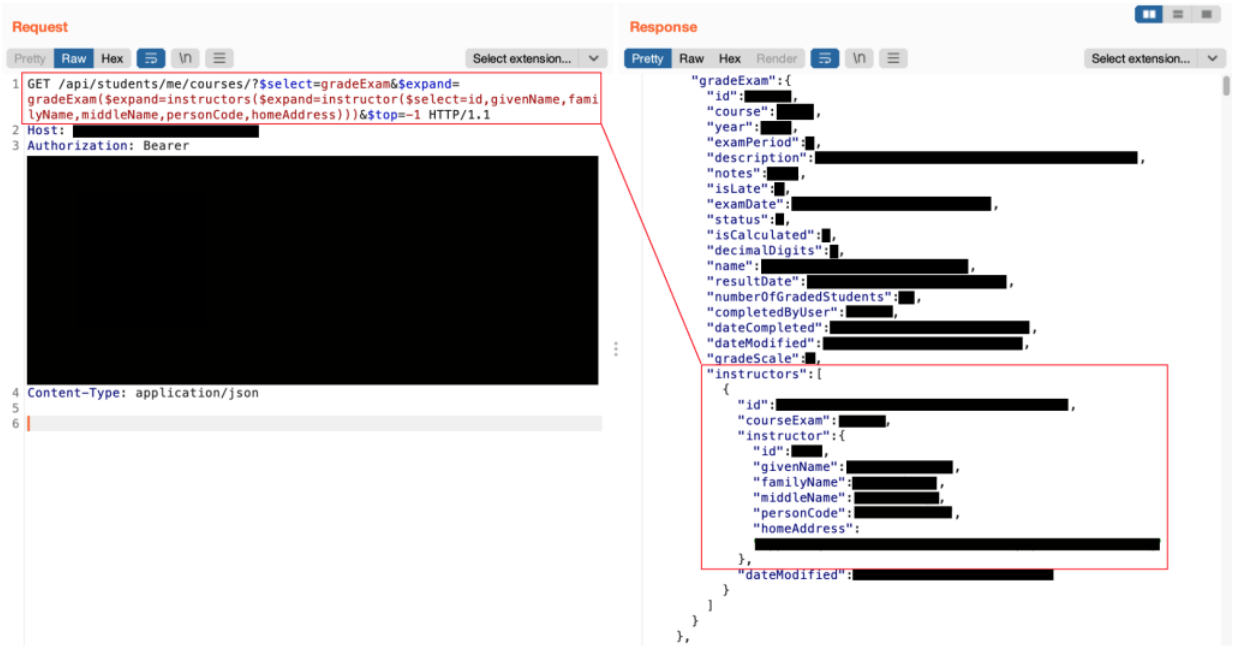

Fig. 1. Obtaining sensitive information (e.g. middle name, Social Security number, and home address) about all instructors in the department.

Remediation

UniverSIS has released a patch for this vulnerability on GitLab. Please update UniverSIS-students to the latest version.

Responsible Disclosure Timeline

Vendor Contact: March 6, 2022
Vendor Fix Released: March 15, 2022
Public Advisory: April 4, 2022
CVE Allocation: April 11, 2022

Previous
Location Privacy in Wireless Networks (for Orwell fans)

Next

CVE-2022-29603: High-Severity SQL Injection Vulnerability in UniverSIS