# Internet2 Incident Report Form

|  |  |
| --- | --- |
| Incident #: | **2017-08-02-01** |
|  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Internet2 Incident Report | | | | | |
| Incident Team Leader’s Information | | | | | |
| Date/Time of Report | 2017-08-15 | | | | |
| First Name | Nicholas | | | | |
| Last Name | Roy | | | | |
| Title/Position | Director of Technology and Strategy, InCommon | | | | |
| Work Email Address & Phone | Email:nroy@internet2.edu | | | | Phone:+1 720 379 9679 |
| Reported Incident Information | | | | | |
| Initial Report Filed With (Organization) | *InCommon Operations* | | | | |
| Start Date/Time | 2017-08-01 15:05 EDT | | | | |
| Incident Location | Ann Arbor, MI | | | | |
| Incident Point of Contact (if different than above) | *Nicholas Roy, IJ Kim* | | | | |
| Possible Compromise of Corporate Data? | There was no possible compromise of corporate data. There is a small chance that a malicious user could attempt to submit invalid Service Provider (SP) SAML metadata, but two duplicate human-based checks in the system, one for Site Administrators and one for InCommon Staff should prevent any such submission from being successful. | | | | |
| Possible Compromise of Personally Identifiable Information (PII)? | If a malicious user successfully submitted false SP metadata and somehow convinced both a Site Administrator and the InCommon RA staff to approve the submission of this metadata, the user could set up an SP that could receive user attribute information from users, but only if users could be tricked into accessing the malicious SP. The chances of all of these steps succeeding is incredibly small given manual check processes in place on submission of / approval of metadata by delegated administrators. Further, since only existing SP metadata may be modified by delegated admins, the chance that a user or SP administrator would notice the replacement of good SP metadata with bad is very high. For this reason we believe that no malicious users ever exploited this vulnerability. | | | | |
| Incident Type | Potential to inject malicious SP metadata into the InCommon federation | | | | |
| US-CERT Category | Unauthorized access | | | | |
| US-CERT Submission Number |  | | | | |
| Description | On August 1, 2017, a delegated SP administrator at a US university discovered that they could access the Site Administrator login URL with only the federated username of a delegated admin, but no password. Delegated admins normally would not use this URL, and the delegated admin had discovered it. Once in the system, the delegated admin could request that the Site Admin make changes to SP metadata to which the delegated admin had been granted access. If the changes were approved by the Site Admin, they would then be sent to the InCommon RA staff for final approval before publication. The delegated administrator contacted InCommon operations staff, and staff immediately patched the Federation Manager database to prevent unauthorized access. | | | | |
| Additional Support Action Requested | We immediately engaged the InCommon Federation Manager software development team to create a software patch to prevent delegated admins from being created with null password values in the future. This patch was released in production at 15:00 EDT on August 2, 2017 | | | | |
| Method Detected | User notification | | | | |
| Number of Hosts Affected | 1 | | | | |
| Department Impact | Internet2 Trust and Identity Services, Internet2 Technical Services Group | | | | |
| Status | Resolved | | | | |
| Systems Involved (list all relevant details including role in the incident) | | | | | |
| IP Address / Range | | Host Name | Operating System | Comments | |
| 207.75.164.123 | | service1.internet2.edu | Linux | Federation Manager application server | |
|  | |  |  |  | |
| Notes / Additional Information: | | | | | |
| Metrics | | | | | |
| Action Description | 1. *Production FM database patched to create random invalid password hash values for all delegated users with existing null values* 2. *FM application code modified to create delegated admin users with random invalid password hash values* 3. *Notification sent to* [*inc-ops-notifications@incommon.org*](mailto:inc-ops-notifications@incommon.org) *mailing list* | | | | |
| Response time from initial report | 16 hours | | | | |
| Detection and Analysis Time | 5+ years (the bug was created when InCommon switched from use of passwords for delegated administrators to use of federated credentials, and was not detected until this incident. That change was made before we started tracking and publishing changes to the Federation Manager, at: https://spaces.internet2.edu/display/INCSWDEV/Release+Notes) | | | | |
| Containment, Eradication, and Recovery Time | 4 hours | | | | |
| Post-Incident Activity Time | 10 hours (additional software development, security incident response) | | | | |
| Notification of 3rd Parties Time | 7 hours | | | | |
| Total Time Involved | 23 hours | | | | |
| Entities Notified | InCommon operations notifications list | | | | |
| Resolution | Software patched, risk assessment and internal review of incident, low risk of exploit determined. | | | | |

|  |
| --- |
| Objective Summary of Incident |

|  |
| --- |
| This was a low risk unauthorized access issue in a software product developed and maintained using a small fraction of a single FTE for many years. The security issue occurred because of an attempt to use a complex and non-deterministic hybrid authentication model with limited resources for implementation and no peer review. It is not surprising that this happened, and is a reason to continue the recent practice of careful analysis of and requirements documentation of any changes to the Federation Manager software or its hosting environment. Further, it highlights the need to adequately resource software development and operations for this critical infrastructure. |

|  |
| --- |
| Timeline |

|  |
| --- |
| See above |

|  |
| --- |
| After-Action Review (Incident Debrief) |

|  |
| --- |
| What went well:   * Excellent teamwork after initial notification of the event. Rapid response in an appropriate manner. Emergency fixes to database and software carried out carefully, professionally and rapidly.   What did not go well:   * Ideally this security issue should never have been created, but it is understandable how it was created given the constraints.   What can be done to be better prepared and/or prevent this issue in the future:   * Proper continued resourcing of Federation Manager software development and systems infrastructure. The addition of I2 T&I’s new DevOps Manager and Security Lead will help in the future, but are likely not sufficient to address all software regressions of this type. |