## Topic 8

**1 Evan Dunphy**

**A** No NVD score as the attack was a social engineering attack and no other **likely vulnerabilities** were found. For our attack I am giving the social engineering attack a made up NVD score of 3.0.

**B** I’m giving it this a low score because there are 2 points that make this vulnerability harder to exploit. 1. The prior information about the admin and 2. The ability to use the information about the admin to trick the steam support contact person. Very hard to exploit but very high impact.

**1 Dylan Moran**

**2 Group**

Researched the admin to gain information to use.

Contacted steam support.

Used the information about the admin to trick steam support.

Used the steam provided password to gain access to the admin account.

Changed the temporary steam password to a stronger password to gain full control of account and to lock out the admin.

Used the account with the POE2 admin tool to view player information.

Used player information to gain access to the player accounts and items.

**3 Group**

Spoofing – The attacker pretended to be an admin to steam support and when using the admin account.

Tampering –The attacker changed passwords of the admin account and the player accounts.

Information Disclosure –The attacker viewed and stole player information and in game items.

Denial of Service –While the attacker carried out the attack the admin and players were locked out of their accounts.

**4 Evan Dunphy**

Medium - Very Severe Impact but Rare Likelihood.

**4 Dylan Moran**

**5 Evan Dunphy**

Yes they are comparable, the result is not surprising. Due to the nature of the attack I had to make a NVD score up.

**5 Dylan Moran**

## Topic 9

**Evan Dunphy**

**1 in diagram**

**2**

Compensating Controls – Employee training, awareness to mitigate carelessness.

Detective Controls – Logs of login time and location, IDS to detect suspicious activity.

Recovery Controls – None

Corrective Controls – Password resets, reset passwords to stop attackers from using the account.

Preventive Controls - None

Deterrent Controls – no 3rd party connections (Grinding gears didn’t implement), warning and login banners. Stops attackers from gaining access through less secure or easier to exploit 3rd party connections.

**3 in diagram**

## Topic 10

**1 Group**

Compromise Accounts is the most likely vector of attack for our incident.

Reference: Mitre Attack

Available at: <https://attack.mitre.org/techniques/T1586/>

**Evan Dunphy**

**A Individual**

Anomalies in Privileged User Account Activity and Other Log-In Red Flags would be indicators of the attack and indicators of the compromise of the accounts, both admin and the player accounts.

**B Individual**

The normal Events Logins, Logoffs in the %SystemRoot%\System32\winevt\logs directory would contain the evidence of the attack.

**C Individual**

For windows to view the logs use the windows event Viewer in the GUI or command line.

**D Individual**

**To players**

Did you receive any notification of password changes?

How badly was your account affected?

How did you find out your account was affected?

Have you updated your email address and password linked to your account?

Have you enabled MFA or 2FA?

**To admin**

Is your account still active?

Did you receive any notification of password changes from steam?

Are you able to disable the account?

Did you receive any suspicious emails or notifications prior to the attack?

Were you in a certain area during the attack?

Did you notice any suspicious account behaviour?

Did you notice anything different about your account?

**Dylan Moran**

## Topic 11

**Group**

**1** Human error was the root cause of our incident.

**2** To eradicate the root cause I would require more extensive employee training and implement stricter account practices.

**3** None reported that I could find, however similar smaller incidents surely occurred throughout the year.

**A N/a**

**B N/a**

**4 Update Form**

|  |  |  |
| --- | --- | --- |
| Report Type | Date | NIS Reportable Incident |
| First Report  (no later than 72 hours after identifying incident) | 07/02/2025 | Choose an item. |
| Interim Report  (optional) | 08/03/2025 |  |
| Final Report  (no later than 72 hours after resolving incident) | Click here to enter a date. |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Service Provider Details | | | |
| Organization Name | Evan-Dylan-Jacob | | |
| Sector | Recreation | | |
| Contact Person |  | | |
| Role/Title |  | | |
| Phone |  | **Email** |  |
| Availability |  | | |
| Other Interested Parties | Steam. Epic Games. | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Incident Details | | | | | | | | |
| Description  Time/date incident discovered  Time/date incident occurred  Internal reference number  High level description of incident | First being reported in January 2025, Path of Exile, an RPG game, made by Grinding Gears Games, was subjected to hacking. The attacker gained access to an admin account, which allowed them to get into multiple user accounts, with the possibility of modifying accounts or stealing user information. Many valuable items, with some taking 100’s of in-game hours to obtain, have been taken from their accounts. | | | | | | | |
| Service(s) affected | What essential services were affected: No essential services | | | | | | | |
| Nature & Impact | Duration | | | Resolved. Damage may still be ongoing. | | | | |
| Number of Affected Users | | | 66 known PoE2 users possibly more | | | | |
| Nature of Compromise  (authenticity, integrity, availability, confidentiality of data or service) | | | Breach. Stolen Data. | | | | |
| Geographic Spread | | | Worldwide | | | | |
| Cross Border Impact | | |  | | | | |
| Data Loss/Breach | | | User account items taken. Changed passwords. | | | | |
| Material Damage | | |  | | | | |
| Financial Loss | | | Yes. early access, and marketplace items | | | | |
| Reputational Damage | | | Yes. PoE2 loss of reputation. | | | | |
| Risk to Health, Safety or possible loss of life | | | Unknown. People take MMOs very seriously. | | | | |
| Root Cause (if known) | Please tick relevant box | | | | | | | |
| System failure  (e.g. software bug, flawed procedure, hardware failure, etc.) |  | Natural disaster  (e.g. storm, earthquake, etc.) | |  | Human error  (e.g. mistake, negligence, etc.) | |  |
| Malicious action  (e.g. cyber-attack, vandalism, theft, software bug, DDoS attack, etc.) | Checkmark with solid fill | 3rd party failure  (e.g. power cut, internet outage, etc.) | |  | Other  (please provide further detail below) | |  |
| Root Cause narrative:  Threat actor wanted to steal in game items. | | | | | | | |
| Severity | Please tick relevant box | | | | | | | |
| Major Impact | | | | | |  | |
| Moderate Impact | | | | | | Checkmark with solid fill | |
| Minor Impact | | | | | |  | |
| Not Yet Known | | | | | |  | |
| No Impact (report for information only) | | | | | |  | |

|  |  |
| --- | --- |
| Current Situation | |
| Investigation Status | Resolved |
| Actions Taken to mitigate or contain | Security patches and updates to the PoE2 game. Reset admin account passwords and sessions. |
| Expected Time to Resolve | 1 month. |
| Support Required from CSIRT | No |
| Please provide further information: |
| Notifications Issued  (Impacted Parties, Executive Management, Law Enforcement, Data Protection Commissioner) | Victims contacted the support services for the PoE2 game. News reported on online sites and discussed on Youtube and forums. |

|  |  |
| --- | --- |
| Information Sharing | |
| Full Incident Information  (ICT assets affected, IoC’s, etc.) |  |
| Lessons Learned  (e.g. vulnerabilities/weaknesses exposed, new threats identified, inadequate processes/controls, staff awareness training needs, success of business continuity and disaster recovery plans, etc.) | Enable MFA for accounts.  Disconnect 3rd party accounts from admin accounts.  Retrain employees on security practices. |

## Week 12

**Summary Evan Dunphy**

A hack occurred in the PC game Path of Exile 2(PoE2). An attacker stole in game items from at least 66 know victims. The attacker used an admin panel to see player account information to get their login details and then changed their passwords to allow the attacker to login as the victim. The attacker gained access to the admin panel by using an old steam account linked to an admin account of the game PoE2. The attacker gained access to the old steam account through a PoE2 admin’s negligence have an old/unused steam account linked to their PoE2 admin account. The attacker learned of this weakness by using social engineering. First reported in January 2025.

Unusual activity of the administrator account and player reporting lead to the attack being discovered.

The attack has been resolved by resetting the admin account or deleting the account entirely, stopping the attacker from using said account to view and player information. Unfortunately, player items could not be returned to them, but their accounts have been recovered.

To mitigate attacks similar in nature it is suggested to train employees to be more aware of social engineering attacks and better account management practices such as disconnecting accounts from 3rd parties and enabling 2FA or MFA.

C. Due to the attack being a social engineering attack some parts of the report had to be made up instead of using technical information.

D. Next time I would choose an attack with more technical information to report on.

E. No.

Dylan Moran