ACADÉMIE
D'AIX-MARSEILLE
Liberté
Égalité
Fraternité

Direction inter-académique
des systèmes d'Information

Pôle national de compétences
en sécurité des systèmes d'information

Affaire suivie par :
Jean-Louis Brunel
Tél : [redacted]
Mél : [redacted]

Place Lucien Paye
13621 Aix-en-Provence cedex 1

Aix-en-Provence, le 1er décembre 2022

Objet : expertise sur la sécurité du code de Parcoursup

Je soussigné Jean-Louis Brunel,

Ingénieur de recherche de l'Éducation nationale, responsable du pôle national de compétence en sécurité des systèmes d'information depuis 2005, placé sous l'autorité hiérarchique de M. le recteur de l'académie d'Aix-Marseille et placé sous l'autorité fonctionnelle de la direction du numérique éducatif atteste avoir réaliser l'homologation de sécurité de Parcoursup.

Dans cadre, j'ai mené l'étude de risques et divers audits de sécurité sur ce système d'information. Ces différentes prestations m'ont conduit :

- à réaliser des interviews des différentes parties prenantes ;
- à prendre connaissance d'audits effectués par des tiers dont des audits de code ;
- à ausculter l'infrastructure et les applications.

Cette connaissance des aspects liés à la gestion des risques et à la sécurité de Parcousup m'amène aux remarques ou conclusions suivantes relatives à la publication du code de Parcoursup.

La divulgation du code source : un risque à mesurer

Dans un objectif de sécurisation et de réduction des coûts associés à la détection de vulnérabilités, des entreprises et plus récemment certaines administrations ont recours à la « prime aux bogues » ou « bug bounty ».

Cette pratique consiste à recourir à des personnes expérimentées dans le domaine des audits techniques ou tests d'intrusion mais aussi dans le développement applicatif qui vont se livrer à des chasses aux bogues en échange de récompenses.

La chasse aux bogues vient compléter les audits ou tests d'intrusion réalisés en interne ou par des prestataires. À la différence de ces derniers qui révèlent des vulnérabilités à un instant donnée, la chasse aux bogues est conduite dans la durée et au fil de l'eau.

Toutefois, elle constitue une activité externalisée qui comme tout externalisation doit contractuellement être

encadrée pour garantir le respect de la réglementation (art. 32 à 34 du RGPD, L-323-1 du code pénal, L.111-7 du code de la consommation).

L'ouverture des codes sources induit forcément une chasse aux bogues. À la différence du « bug bounty », elle n'est pas encadrée et ouvre la porte à des hackers non éthiques.

Dans la mesure où il n'est pas possible de maitriser le public à qui le code est ouvert, la seule maitrise réside dans la maitrise des portions de code divulguées.

La sécurité par la confidentialité comme moyen de défense en profondeur

Ne pas publier le code source est souvent assimilé à une mauvaise pratique appelée sécurité par l'obscurité.

La sécurité par l'obscurité consiste à considérer que la meilleure et seule façon de se protéger est de se soustraire à la menace en se cachant. Conçue par ses tenants, comme seul moyen de défense pour éviter de mettre en œuvre les mesures de sécurité adéquates, elle est un leurre donnant l'illusion de la sécurité.

Toutefois, il est nécessaire de distinguer dans le code Parcoursup le code qui traduit une procédure administrative du reste du code qui implante des IHM ou des procédures d'échanges avec d'autres systèmes d'information. La non divulgation du code qui ne correspond pas à la traduction informatique des procédures administratives ne peut et ne doit pas être confondue avec la mauvaise pratique que constitue la sécurité par l'obscurité.

Elle répond à plusieurs impératifs :

- prendre en compte le fait que les cyber-attaques sont quasi toujours précédées de phase d'observation et de reconnaissance. La lecture du code constitue aussi une phase de reconnaissance pour un hacker non éthique ;
- ne pas faciliter la tâche des sources de menaces dans leurs investigations pour comprendre le système et acquérir la cible ;
- se préserver à plus long terme, même pour un code assaini ou jugé sain, de la découverte et l'exploitation de failles du jour zéro (Zero day).

De ce point de vue, l'absence de confidentialité de l'intégralité du code qu'implique l'exigence de la transparence, priverait Parcoursup d'un moyen de défense en profondeur qui est un concept qu'on retrouve dans les domaines militaires, industriels et de la sécurité des systèmes d'information.

La divulgation de l'intégralité du code sans apporter davantage quant à la compréhension des procédures administratives, faciliterait la tâche de hackers non éthiques.

Il est donc impératif d'éviter la confusion entre sécurité par l'obscurité et sécurité par la confidentialité.

En l'état actuel, la déficience voire l'obsolescence d'une partie du code de Parcoursup rendent nécessaire cette mesure de sécurité.

L'illusion de la sécurité périmétrique comme mesure de compensation

Les serveurs applicatifs qui déroulent la logique du code de Parcoursup sont implantés sur des réseaux internes protégés des accès directs en provenance d'internet par des équipements de sécurité.

Dans le concept de défense en profondeur, ces équipements de sécurité qui protègent les serveurs applicatifs sont placés :

- à la frontière entre internet et les réseaux internes ;
- successivement entre les réseaux internes eux-mêmes pour assurer un cloisonnement défensif.

Il est possible de prévenir en partie les attaques qui viseraient les faiblesses du code de Parcoursup en configurant

ces équipements pour détecter et stopper ces attaques. Cette pratique s'appelle la défense périmétrique et elle est mise en œuvre de façon rigoureuse sur l'infrastructure Parcoursup.

Cette défense périmétrique présente toutefois un grand nombre de limites :

- Il est possible de leurrer les équipements de défense périmétrique en obfusquant les attaques ;
- les équipements de défense périmétrique peuvent se trouver démunis devant une attaque exploitant une vulnérabilité du jour zéro car ils ne détecteraient pas sa signature ou l'analyse comportementale s'avérerait inopérante,
- **enfin et de façon beaucoup plus grave**, la défense périmétrique peut être assimilée aux remparts des cités antiques ou moyenâgeuses. L'antique légende du cheval de Troie montre qu'il est possible de les contourner, l'absence de défense en profondeur laissant le champ libre à l'assaillant.

Sur ce point, un grand nombre d'entreprises ou d'administrations d'État a déjà vu ses défenses périmétriques contournées et l'assaillant prendre pied sur le réseau interne. Une fois in situ, la connaissance du code en amont va accroitre le temps dont il dispose pour atteindre ses objectifs visés et réduire le temps de de détection et de réaction de l'organisation défensive.

Bien que Parcoursup soit opérateur de service essentiel, la prise en compte d'un contournement des défenses périmétriques est essentielle.

La sécurité par la confidentialité, évoquée supra, participe de la défense en profondeur au même titre que la prise en compte des bonnes pratiques dans le développement, l'audit, le test d'intrusion, la prime aux bogues, les systèmes de gestion des événements et des informations de sécurité (SIEM), …

Parcoursup présente un degré élevé d'attractivité pour des hackers non éthiques qui justifie pour partie sa désignation comme opérateur de service essentiel.

L'attractivité élevée du système d'information Parcoursup exige la mise en œuvre de plusieurs barrières de sécurité indépendantes. La non divulgation du code est constitutive d'une de ses barrières qu'il est déraisonnable d'enlever.

La mise à disposition du code source : un processus à gérer

Enfin, il est nécessaire d'apprécier l'ouverture du code source à l'aune de l'industrialisation du développement logiciel.

La mise à disposition du code source au public ne consiste pas seulement à le déposer sur un dépôt de développement logiciel accessible au grand public. Dans le cadre de l'industrialisation du développement logiciel, les découvertes de vulnérabilités doivent être gérées dans un processus de maintenance corrective ou évolutive.

Le laps de temps s'écoulant entre la publication d'une vulnérabilité et sa correction crée une fenêtre d'exposition à des attaques. Certes la durée de cette fenêtre d'exposition peut être réduite par la mise en œuvre de mesures de défense périmètre mais il faut souligner qu'elle ne sera jamais égale à zéro.

Par essence, les publications des internautes sur des vulnérabilités d'un système d'information ne peuvent pas intégrer un processus d'industrialisation et sont constitutives, sui generis d'une vulnérabilité. **Dans le cas de Parcoursup, cette divulgation correspond à une prise de risques qui n'apporte rien au regard de la nécessaire transparence vis-à-vis des usagers.**

Attestation établie le 1er décembre à Aix-en-Provence

Jean-Louis Brunel
Responsable du PNSSI – DNE Socle 4