Inzicht tonen in de impact van de kwetsbaarheden die wij hebben gevonden.

Wij gaan een kwetsbaarheid binnen een verouderde versie van Chamilo exploiteren.

Er is een functionaliteit in Chamilo genaamd "Chamilo Rapid" die automatisch PowerPoints omzet naar cursussen. Deze functie kun je oproepen zonder account en er zit hier een kwetsbaarheid in die toestaat om een shell te openen. Dit kan catastrofaal zijn voor het volledige platform, omdat het zorgt voor volledige toegang tot de server zelf extern, bijvoorbeeld door middel van een reverse shell.

Zo'n diepe toegang is echt een groot probleem voor een bedrijf. Hier zijn een aantal mogelijke gevolgen:

1. Dit kan de correcte werking van het platform beïnvloeden, en dus meerdere lessen en docenten het moeilijk maken om hun les verder te geven.
    - Dit zal voor problemen en ongemak zorgen maar is niet per se catastrofaal.
2. In het geval dat de database niet correct beveiligd is en niet op een geïsoleerde machine draait, zal er ook toegang zijn tot alle gegevens van docenten en studenten.
    - Dit zal ervoor zorgen dat het bedrijf in ernstige onomkeerbare problemen komt als er gegevens van studenten en docenten worden verspreid.
3. Er kan valse informatie worden verspreid die ervoor zorgt dat studenten en docenten de verkeerde informatie bezitten.
    - Dit zal als gevolg hebben dat er een ernstig verlies in vertrouwen zal zijn voor zowel studenten als docenten in het platform.

Niet al deze consequenties zijn even erg. Maar het feit dat er een mogelijkheid is voor een datalek, betekent dat dit probleem echt serieus genomen zal moeten worden.

We hebben al wat besproken over de ernst van dit probleem. Maar hoe kan dit aangepakt worden? Er zijn 2 opties.

De kwetsbaarheid wordt ontdekt VOORDAT deze kan worden misbruikt, of misbruikt is.

- In dit geval is het zo simpel als het controleren op nieuwe versies van Chamilo. In het geval er nog geen update is die dit oplost, moet de kwetsbare service uitgeschakeld worden en dit probleem gemeld worden.

De kwetsbaarheid wordt gebruikt om één van bovenstaande gevolgen waar te maken.

- In dit geval is het niet zo simpel. Er zal direct damage control moeten worden toegepast.
- De server zal moeten worden afgezonderd van het internet om externe toegang af te sluiten.
- Dan zal deze moeten worden onderzocht op eventuele permanente veranderingen.
- Na het vinden van de kwetsbaarheid zal deze service moeten worden uitgeschakeld en zal dit moeten worden gemeld aan de uitgever.
- Er zal ook een aankondiging moeten worden gemaakt dat het platform niet meer beschikbaar is en dat er aan gewerkt wordt.
- Er moet ook een interne analyse worden gedaan om te zien wat de schade is en ook actie worden ondernomen om deze schade zo veel mogelijk te minimaliseren.

Deze exploit zal enorm veel tijd vragen van het team om het systeem terug in een veilige status te brengen vanwege de hoeveelheid schade die kan worden aangericht hierdoor.

Wij gaan ook een kwetsbaarheid binnen een verouderde versie van WooCommerce exploiteren.

Als je bepaalde headers aanpast in een verzoek, kun je toegang krijgen tot de WordPress API aan de hand van je nieuw account met admin rechten kunt toevoegen aan de WordPress site en dus volledige toegang kunt krijgen tot de WordPress pagina.

Deze exploit kan enorm gevaarlijk zijn omdat het gemakkelijk onder de radar kan gebeuren. Bijvoorbeeld:

1. Door subtiel de webpagina aan te passen, kun je gebruikers foutieve informatie geven.
    - Dit zal als gevolg hebben dat je klanten zeer ontevreden zullen zijn.
2. "Defacing" kan ook worden gebruikt. Dit is minder subtiel maar zal ook het imago van de website of het bedrijf schaden door de webpagina te vullen met irrelevante, soms ongepaste beelden en berichten.
    - Dit zal als gevolg hebben dat je klanten zullen schrikken en respect voor het bedrijf zullen verliezen.
3. Je kunt ook phishing gebruiken om bijvoorbeeld de inloggegevens door te sturen naar één van jouw servers voordat ze naar de effectieve, correcte inlogserver gaan.
    - Dit zal de wachtwoorden en e-mailadressen van klanten in gevaar brengen, en kan catastrofaal zijn voor het vertrouwen van de klanten. En zelf onomkeerbare schade doen aan het bedrijf. Want er kunnen niet alleen inloggegevens worden gelekt maar ook bankgegevens bijvoorbeeld.

Hoe valt dit op te lossen? Net zoals bij Chamilo zijn er 2 opties.

De kwetsbaarheid wordt ontdekt VOORDAT deze kan worden misbruikt, of misbruikt is.

- In dit geval is het zo simpel als het controleren op nieuwe versies van de WordPress API. In het geval er nog geen update is die dit oplost, moet de website uitgeschakeld worden en dit probleem gemeld worden.

De kwetsbaarheid wordt gebruikt om één van bovenstaande gevolgen waar te maken.

- In dit geval is het niet zo simpel. Er zal direct damage control moeten worden toegepast.
- De server zal moeten worden afgezonderd van het internet om externe toegang af te sluiten.
- De admin-accounts zullen direct moeten worden gecontroleerd zodat het probleem gevonden wordt.
- Dan zal de server moeten worden onderzocht op eventuele permanente veranderingen en dat moet worden teruggedraaid naar een versie van vóór de aanval.
- Na het vinden van de kwetsbaarheid zal dit admin-account direct moeten worden uitgeschakeld.
- Er moet zeker een interne analyse worden uitgevoerd om te zien wat de schade is en ook actie worden ondernomen om deze schade zo veel mogelijk te minimaliseren door bijvoorbeeld klanten die hierdoor beïnvloed waren op de hoogte te brengen.

Zolang er backups van de website bestaan zal deze exploit relatief weinig tijd vragen van het team om het systeem terug in een veilige status te brengen. Maar als er een soort phishing attack heeft plaatsgevonden zal de schade aan de klanten hun gegevens bijna onmogelijk te herstellen zijn.