Introductie

In 2012 bracht BIT voor het eerst een transparantierapport uit. Het doel van dit rapport is om inzicht te geven in het aantal bevragingen (door opsporingsinstanties) naar persoonsgegevens van klanten van BIT, het aantal notice-and-take-down-verzoeken, en hoe veel Responsible Disclosure-meldingen BIT heeft ontvangen. In dit rapport delen we de informatie over het jaar 2025.

We laten deze gegevens zien omdat we het belangrijk vinden om eerlijk te zijn, vooral met alle veranderingen en ontwikkelingen op het gebied van privacy. We willen onze klanten en andere mensen die geïnteresseerd zijn laten weten wat er gaande is. Om eventuele patronen of ontwikkelingen te laten zien, hebben we de cijfers van 2021 tot en met 2025 in dit verslag gezet.

In dit rapport is per categorie te lezen hoeveel klachten, verzoeken of meldingen we hebben ontvangen en hoe we ermee zijn omgegaan.

Inhoudsopgave

1 Verstrekking van persoonsgegevens

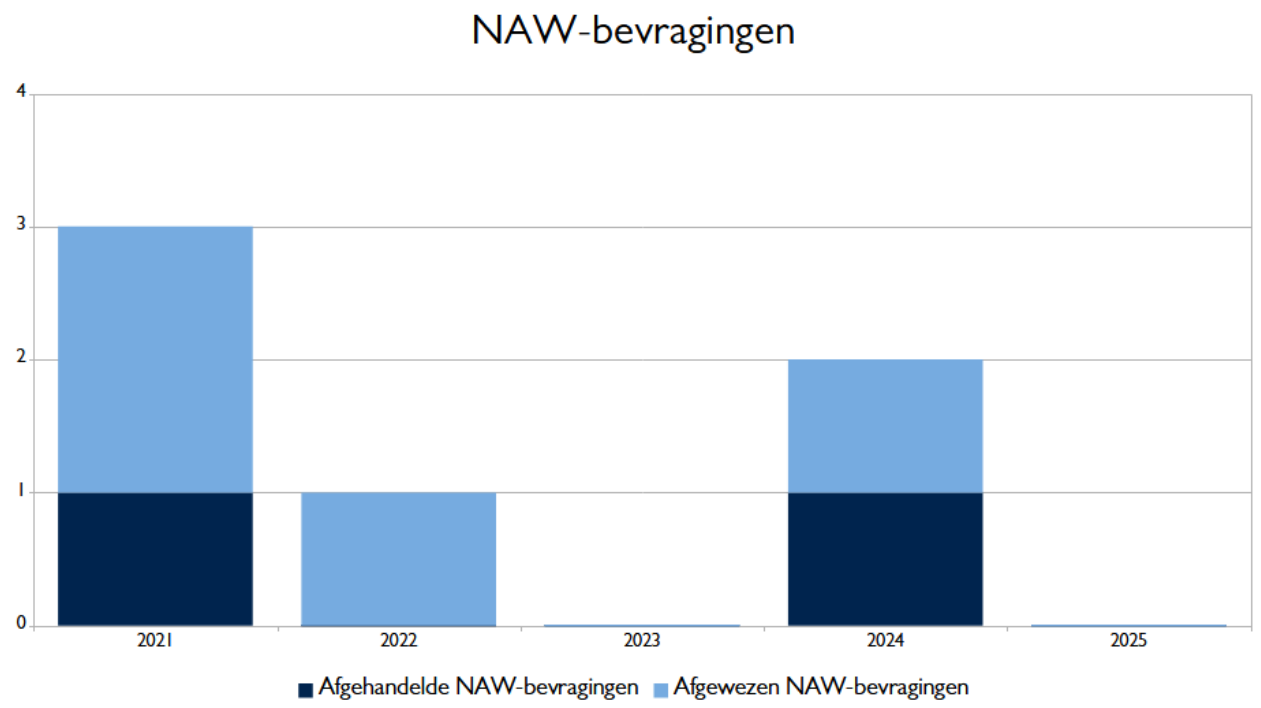
De sectie 'Verstrekking van persoonsgegevens' is opgedeeld in vier subcategorieën, te weten NAW-bevragingen, melding van inbreuk in verband met persoonsgegevens, tapbevelen, en overige. Per subcategorie wordt weergegegven hoe veel verzoeken BIT heeft ontvangen in 2025 en hoe deze zijn afgehandeld.

1.1 NAW-bevragingen

In de tabel hieronder ziet u het aantal ontvangen verzoeken voor het verstrekken van persoonsgegevens van klanten van BIT aan opsporingsinstanties. Ook staat aangegegeven hoe vaak we wel of niet aan dat verzoek hebben voldaan.

	2021	2022	2023	2024	2025
Afgehandelde NAW-bevragingen	1	0	0	1	0
Afgewezen NAW-bevragingen	2	1	0	1	0
Totaal	3	1	0	2	0

In onderstaande grafiek hebben we het aantal NAW-bevragingen van de afgelopen vijf jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.



1.2 Melding van inbreuk in verband met persoonsgegevens

BIT is wettelijk verplicht om melding te maken van inbreuk(en) op persoonsgegevens. In 2025 was er geen aanleiding tot dergelijke melding(en).

	2021	2022	2023	2024	2025
Meldingen inbreuk persoonsgegevens	0	0	0	1	0

1.3 Tapbevelen

De Nationale Politie, FIOD-ECT, Nederlandse Arbeidsinspectie, IOD, AID, AIVD en MIVD hebben het recht op bij een provider een bevel neer te leggen voor (af)tappen, zoals e-mail of IP-taps. Hieronder staat een tabel met het aantal tapbevelen dat BIT heeft ontvangen in de afgelopen vijf jaar.

	2021	2022	2023	2024	2025
Ontvangen tapbevelen	0	0	0	2	0

1.4 Overige

De categorie 'overige' binnen 'verstrekking van persoonsgegevens' omvat alle verzoeken/bevelen/bevragingen die niet binnen de eerder genoemde categorieën vallen. In 2025 heeft BIT geen overige bevelen ontvangen.

2 Take-down-verzoeken

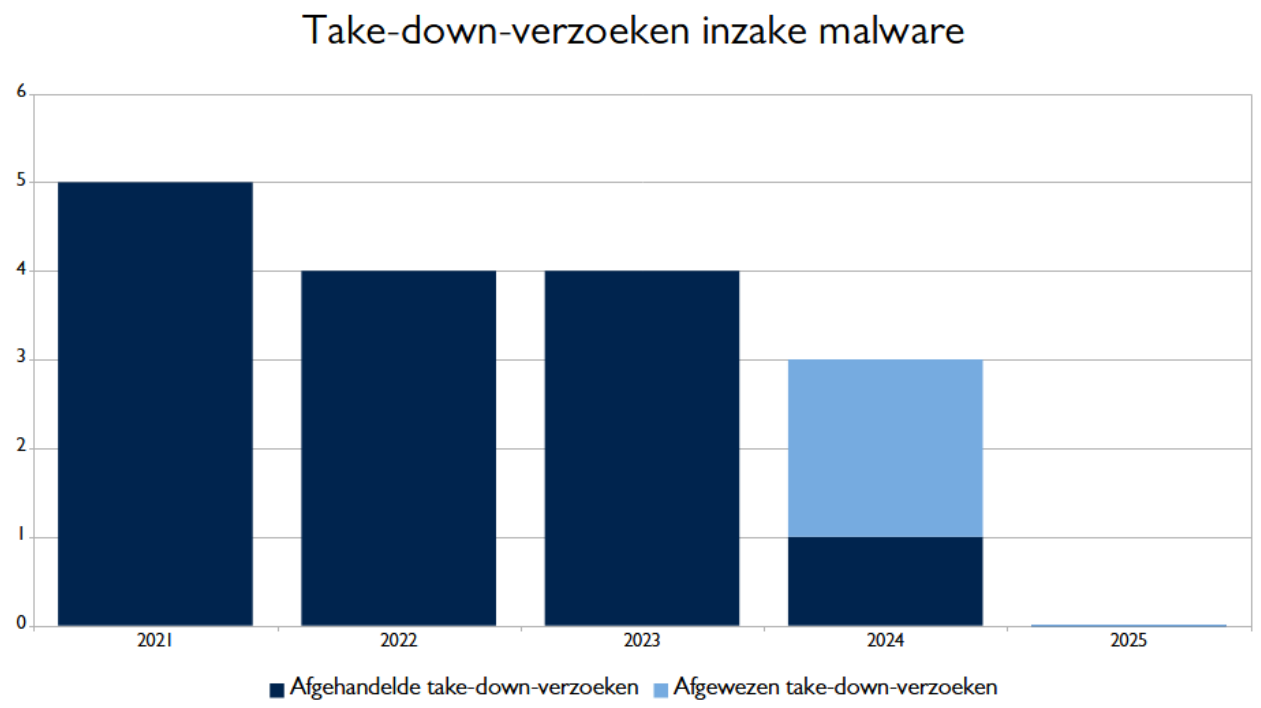
De sectie 'Take-down-verzoeken' is opgedeeld in vijf subcategorieën, te weten take-down-verzoeken inzake malware, copyrightschending, phishing, kinderporno en terroristische content. Per subcategorie wordt weergegegven hoe veel verzoeken BIT heeft ontvangen in 2025 en of deze verzoeken zijn afgehandeld of afgewezen.

2.1 Take-down-verzoeken inzake malware

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen vijf jaar heeft ontvangen vanwege het (vermeend) hosten van malware, inclusief of deze verzoeken zijn afgehandeld of afgewezen.

	2021	2022	2023	2024	2025
Afgehandelde take-down-verzoeken	5	4	4	1	0
Afgewezen take-down-verzoeken	0	0	0	2	0
Totaal	5	4	4	3	0

In onderstaande grafiek hebben we het aantal take-down-verzoeken met betrekking tot malware van de afgelopen vijf jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.



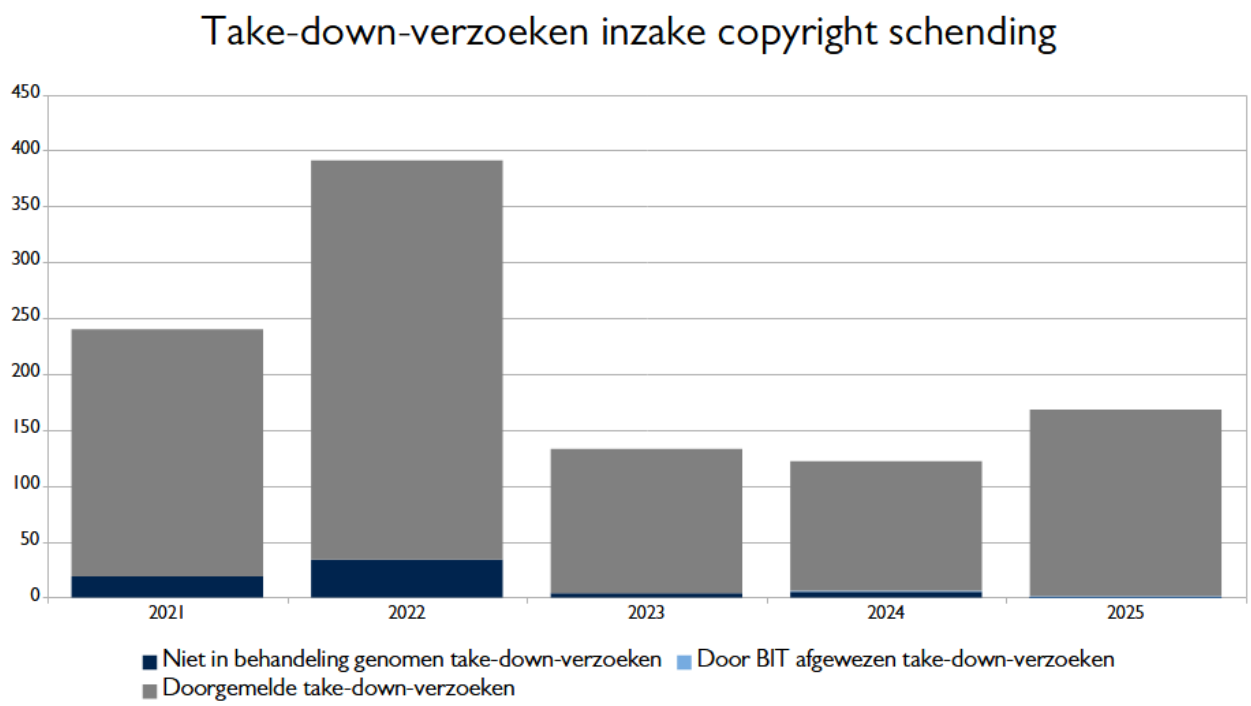
2.2 Take-down-verzoeken inzake copyrightschending

In het transparantierapport van 2013 heeft BIT voor het eerst cijfers gedeeld over ontvangen en afgehandelde notice-and-take-down-verzoeken met betrekking op (vermeende) copyrightschending.

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen vijf jaar heeft ontvangen vanwege (vermeende) copyrightschending, of deze verzoeken zijn afgehandeld, afgewezen of doorgemeld.

	2021	2022	2023	2024	2025
Niet in behandeling genomen take-down-verzoeken	19	34	4	5	0
Door BIT afgewezen take-down-verzoeken	0	0	0	1	1
Doorgemelde take-down-verzoeken	221	357	129	116	167
Totaal	240	391	133	122	168

In onderstaande grafiek hebben we het aantal take-down-verzoeken met betrekking tot copyrightschending van de afgelopen vijf jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen

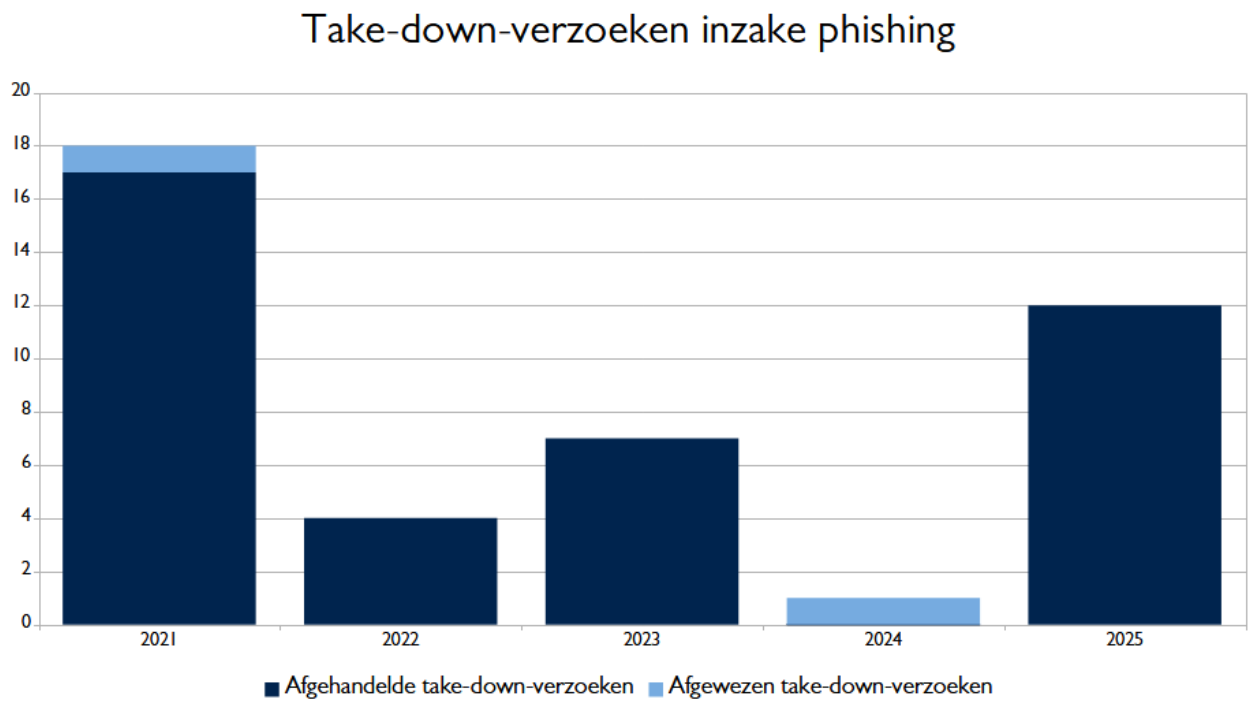


2.3 Take-down-verzoeken inzake phishing

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen vijf jaar heeft ontvangen inzake phishingsites, inclusief of deze verzoeken zijn afgehandeld of afgewezen.

	2021	2022	2023	2024	2025
Afgehandelde take-down-verzoeken	17	4	7	0	12
Afgewezen take-down-verzoeken	1	0	0	1	0
Totaal	18	4	7	1	12

In onderstaande grafiek hebben we het aantal take-down-verzoeken met betrekking tot phishing van de afgelopen vijf jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.



2.4 Take-down-verzoeken inzake kinderporno

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen vijf jaar heeft ontvangen inzake kinderporno, inclusief of deze verzoeken zijn afgehandeld of afgewezen.

	2021	2022	2023	2025	2025
Afgehandelde take-down-verzoeken	0	0	0	0	0
Afgewezen take-down-verzoeken	0	0	0	0	0
Totaal	0	0	0	0	0

2.5 Take-down-verzoeken inzake terroristische content

Vanaf juni 2022 is er een Europese verordening van toepassing die regels vaststelt om de verspreiding van online terroristisch materiaal tegen te gaan. In Nederland worden deze regels gehandhaafd door de ATKM.

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT sinds 2022 heeft ontvangen inzake terroristische content, inclusief of deze verzoeken zijn afgehandeld of afgewezen.

	2022	2023	2024	2025
Afgehandelde take-down-verzoeken	0	0	0	0
Afgewezen take-down-verzoeken	0	0	0	0
Totaal	0	0	0	0

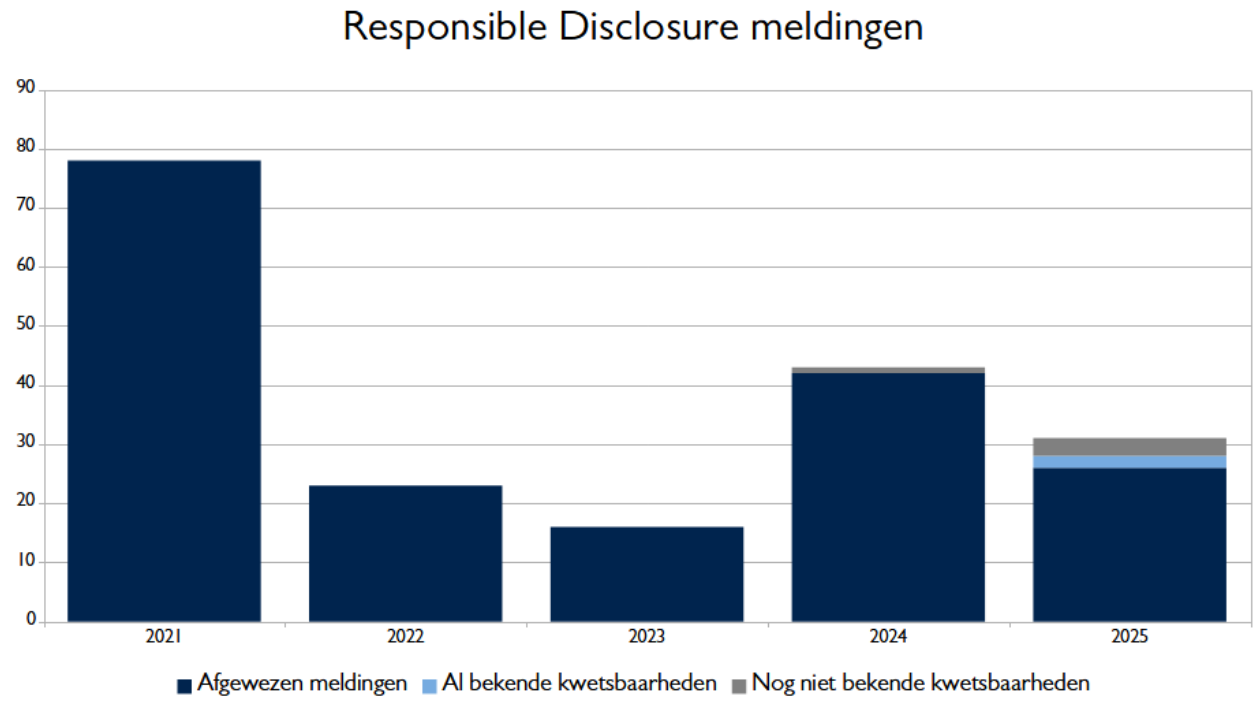
3 Responsible Disclosure

In onderstaande tabel wordt aangegeven hoe veel Responsible Disclosure-meldingen er bij BIT zijn gedaan. In dit overzicht hebben we onderscheid gemaakt in afgewezen meldingen, reeds bekende kwetsbaarheden en nog niet bij ons bekende kwetsbaarheden.

In 2025 hebben we zes (6) Responsible Disclosure-meldingen doorgestuurd naar klanten van BIT

	2021	2022	2023	2024	2025
Afgewezen meldingen	78	23	16	42	26
Al bekende kwetsbaarheden	0	0	0	0	2
Nog niet bekende kwetsbaarheden	0	0	0	1	3
Totaal	78	23	16	43	31

In onderstaande grafiek hebben we het aantal Responsible Disclosure-meldingen van de afgelopen vijf jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.



4 Conclusies en opmerkingen

In het jaar 2025 heeft BIT geen verzoeken ontvangen voor het verstrekken van persoonsgegevens van klanten aan opsporingsinstanties. Dit geldt zowel voor NAW-bevragingen, waarbij geen enkel verzoek werd ingewilligd of afgewezen, als voor tapbevelen, waarbij geen enkel bevel werd ontvangen. Ook waren er er geen meldingen van inbreuken op persoonsgegevens. Het lage aantal bevragingen omtrent persoonsgegevens is te wijten aan het feit dat BIT geen diensten aan particulieren levert.

Sinds 2023 wordt er ook over de categorie 'Overige' gerapporteerd. Deze categorie bestaat al langer, maar 2023 was het eerste jaar waarin BIT vorderingen binnen deze categorie heeft ontvangen. In 2025 kwamen er in deze categorie geen vorderingen binnen.

Het aantal meldingen van schendingen van auteursrechten (copyrightmeldingen) is gestegen ten opzichte van 2024. Dit zijn voor het overgrote deel verzoeken die doorgemeld zijn aan onze klanten.

Sinds 2019 hebben we besloten om geen vergoeding meer te vermelden in ons Responsible Disclosure-beleid, en sindsdien is het aantal meldingen ook lager geworden. We ontvangen wel nog relatief veel meldingen over zaken die bewust openbaar zijn, waar bewuste keuzes zijn gemaakt voor instellingen, of waar kwetsbaarheden zijn vastgesteld uit versienummers terwijl er bijvoorbeeld backports zijn gebruikt. Daarnaast krijgen we ook meldingen over systemen die zijn uitgesloten in ons Responsible Disclosure-beleid, zoals klantsystemen. Deze meldingen sturen we wel door naar de betreffende klant.

In 2025 hebben we drie keer een bounty uitgekeerd naar aanleiding van een Responsible Disclosure-melding. Het betrof meldingen waarbij de onderzoeker aantoonde dat er mogelijk informatie kon worden prijsgegeven of dat invoer onvoldoende werd gevalideerd.

De eerste melding betrof een publiek toegankelijke Grafana-instance waarin Grafana's eigen metrics zichtbaar waren. Deze instance toonde geen klantgegevens of andere gevoelige informatie, toch hebben we de toegang verder beperkt om onbedoelde inzage en verdere meldingen te voorkomen.

De tweede melding ging over het tonen van stacktraces vanuit een Tomcat-omgeving. In deze stacktraces stond geen gevoelige informatie, het kan informatie geven aan aanvallers om gericht aanvallen op te zetten. Daarnaast staat het op de lijst van ethische hackers om over te melden.

De derde en laatste melding betrof een reflected Cross-Site Scripting (XSS)-kwetsbaarheid waarbij de target-URL van een redirect kon worden beïnvloed. Hoewel er geen directe impact op klantgegevens was, kan een dergelijke kwetsbaarheid misbruikt worden door middel van gerichte phishing.