



openbaren. Ik heb ervoor gekozen niet dat woord weg te halen, omdat dan de verdenking wordt dat we iets te verbergen hebben. Voor wie het interesseert: in de duidingsrapportage staat per bevinding wat we ermee doen of hoe wij er tegenaan kijken.

Voor de toekomst om dit soort meldingen niet onnodig te vertragen is voor coronamelder (en straks de app2) het logische adres om naartoe te mailen: [5.1.5@coronamelder.nl](mailto:5.1.5@coronamelder.nl) dan komt het bij zowel [5.1.2e](mailto:5.1.2e) als mij uit. Misschien ook handig mijn telefoonnummer te hebben (in het kader van bellen is sneller): [5.1.2e](tel:5.1.2e).

Nogmaals dank voor de scherpte! Iedere melding is nuttig, want er wordt met veel kritische ogen naar ons gekeken. Dus mocht je wat zien of iets een zorg geven: laat het weten.



--

Hartelijke groet,

5.1.2e  
5.1.2e

Ministerie van Volksgezondheid, Welzijn en Sport

Op 30-09-2020 om 12:31 schreef [5.1.2e](mailto:5.1.2e):

Dag [5.1.2e](mailto:5.1.2e)

Hierbij de NCSC melding.

@CC-geadresseerden: het betreft een actie om deze info openbaar te maken. Minder handig is dat die openbaar gemaakte info nog steeds gelabeld is als "vertrouwelijk".

Met vriendelijke groet,

5.1.2e 5.1.2e  
5.1.2e

**Ministerie van Volksgezondheid, Welzijn en Sport**  
**Directie Informatiebeleid - CIO**

5.1.2e  
Parnassusplein 5 | Den Haag | 5.1.2e  
Postbus 20350 | 2500 EJ | Den Haag  
5.1.2e

T [5.1.2e](mailto:5.1.2e)  
[5.1.2e@minvws.nl](mailto:5.1.2e@minvws.nl)  
<http://www.minvws.nl/>

**Zorg gaat iedereen aan.**

---

**Van:** [5.1.2e](mailto:5.1.2e) <[5.1.2e@minvws.nl](mailto:5.1.2e@minvws.nl)>  
**Verzonden:** woensdag 30 september 2020 12:16  
**Aan:** [5.1.2e](mailto:5.1.2e) <[5.1.2e@minvws.nl](mailto:5.1.2e@minvws.nl)>  
**CC:** [5.1.2e](mailto:5.1.2e) <[5.1.2e@minvws.nl](mailto:5.1.2e@minvws.nl)>; [5.1.2e](mailto:5.1.2e) <[5.1.2e@minvws.nl](mailto:5.1.2e@minvws.nl)>  
**Onderwerp:** FW: Melding vertrouwelijke gegevens op GitHub CoronaMelder  
**Urgentie:** Hoog

Goedemiddag [5.1.2e](mailto:5.1.2e)

5.1.2e is op 5.1.2e afwezig maar, omdat het 'mogelijk' om gerubriceerde informatie gaat die gecompromitteerd is, vind ik het belangrijk dat dit meteen opgepakt wordt. Vandaar even mijn vraag wie kan dit nu oppakken en ik maar even escaleer naar jou.

Belangrijkste is vaststellen wat er daadwerkelijk aan de hand is, misschien niets, en mocht er wel informatie gecompromitteerd zijn direct maatregelen treffen om het incident in te perken. Kun jij mij s.v.p. informeren over het onderzoek en eventuele (nood)maatregelen mochten die nodig zijn ? Dank.

Met vriendelijke groet,

5.1.2e 5.1.2e  
5.1.2e



Ministerie van Volksgezondheid,  
Welzijn en Sport

Directie Bestuurlijke en Politieke Zaken 5.1.2e  
Parnassusplein 5 | 2511 VX | Postbus 20350 | 2500 EJ DEN HAAG  
5.1.2e  
@ 5.1.2e @minvws.nl

5.1.2e 5.1.2e +31 5.1.2e |  
@ 5.1.2e @minvws.nl

**Bij het Ministerie van VWS geldt een legitimatieplicht (Rijkspas) en/of identificatieplicht voor toegang tot het ministerie.**

Van: 5.1.2e <5.1.2e @minvws.nl>

Verzonden: woensdag 30 september 2020 11:40

Aan: 5.1.2e <5.1.2e @minvws.nl>

CC: 5.1.2e <5.1.2e @minvws.nl>

Onderwerp: FW: Melding vertrouwelijke gegevens op GitHub CoronaMelder

Urgentie: Hoog

Hoi 5.1.2e

Is deze melding vanuit het NCSC bij jou binnengekomen ? Wellicht kun je onderzoeken wat er precies gebeurd is en of dit een compromittering van gerubriceerde informatie is ?

Met vriendelijke groet,

5.1.2e 1.2e  
5.1.2e

Directie Bestuurlijke en Politieke Zaken, 5.1.2e  
Parnassusplein 5 | 2511 VX | Postbus 20350 | 2500 EJ DEN HAAG  
+31 ( 5.1.2e  
@ 5.1.2e @minvws.nl

Verzonden met BlackBerry

Van: 5.1.2e @mindef.nl <5.1.2e @mindef.nl>

Datum: woensdag 30 sep. 2020 11:32 AM

Aan: 5.1.2e <5.1.2e @minvws.nl>, 5.1.2e <5.1.2e @minvws.nl>

Kopie: 5.1.2e @mindef.nl <5.1.2e @mindef.nl>

Onderwerp: FW: Melding vertrouwelijke gegevens op GitHub CoronaMelder

Collega's,

Zie hieronder van een melding van onze collega's van DCSC.  
Sourcecode van de coronadashboard en pentestrapportage staat volgens onderstaande info openbaar terwijl de rubricering van de stukken op confidentieel staan.

NCSC heeft de melding als het goed is ook naar jullie doorgezet.  
Indien nog andere detail info gewenst is kan eventueel contact gelegd worden met mijn collega in cc.

Gezien de situatie waarin we ons als BV NL bevinden is het wellicht raadzaam om dit na te gaan om eventuele schade te voorkomen.

Gr 5.1.2e

---

**Van:** 5.1.5 <[redacted]@mindef.nl>

**Verzonden:** woensdag 30 september 2020 10:32

**Aan:** 5.1.2e <[redacted]@ncsc.nl> <[redacted]@ncsc.nl>

**CC:** 5.1.2e <[redacted]@mindef.nl> 5.1.2e <[redacted]@mindef.nl> 5.1.2e <[redacted]@mindef.nl>

**Onderwerp:** Melding vertrouwelijke gegevens op GitHub CoronaMelder

Goedemorgen,

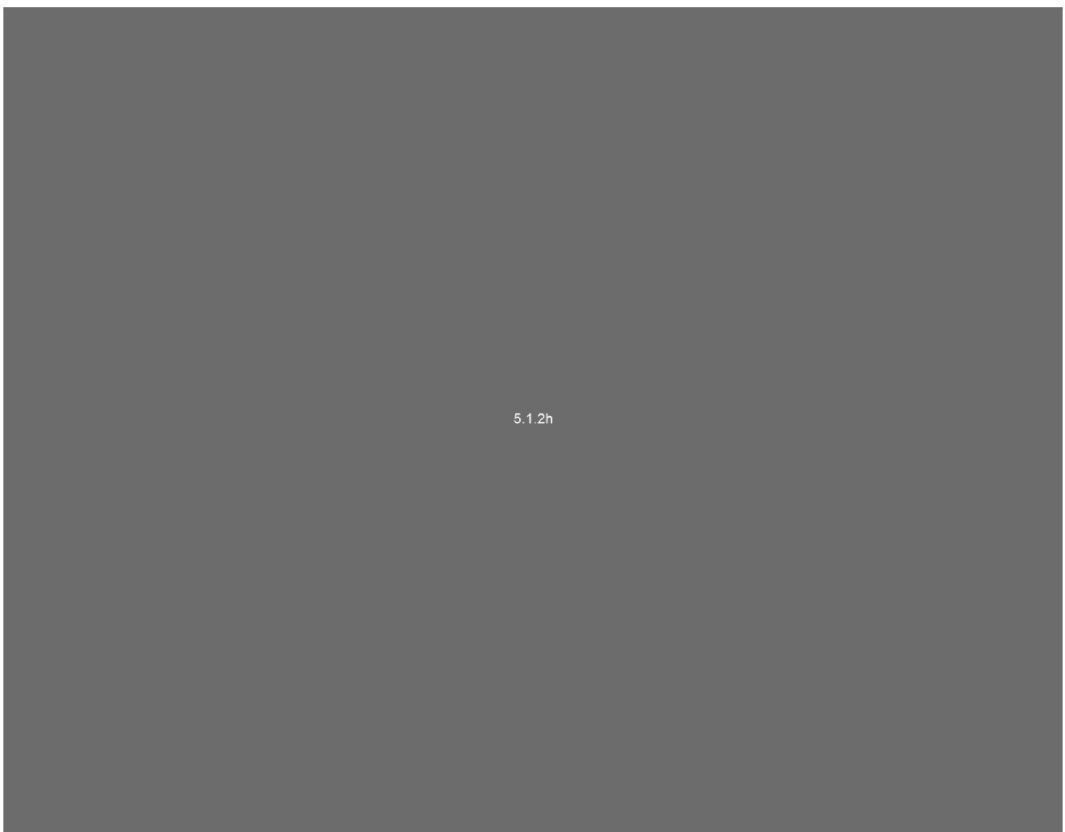
Zojuist hebben wij de melding binnen gekregen over vertrouwelijke informatie van de CoronaMelder App. Op de Github van het Minvws staan diverse documenten van het COVID19 dashboard en de CoronaMelder App.

Op de hieronder bijgevoegde link is de rapportage van de penetratietest te vinden:

5.1.2h

Overige documenten:

5.1.2h



5.1.2h

Met vriendelijke groet,

5.1.2e

5.1.2e

5.1.2e

**Ministerie van Defensie**

Camp New Amsterdam | Dolderseweg 34, 3712BR Huis Ter Heide |  
Postbus 90125 | 5.1.2e 3509BB Utrecht

5.1.2e

V 5.1.2e  
M 5.1.2e  
E 5.1.2e [@mindef.nl](mailto:)  
I [www.defensie.nl/dmo](http://www.defensie.nl/dmo)

5.1.2e

**JIVC** hét IT-bedrijf van Defensie



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.