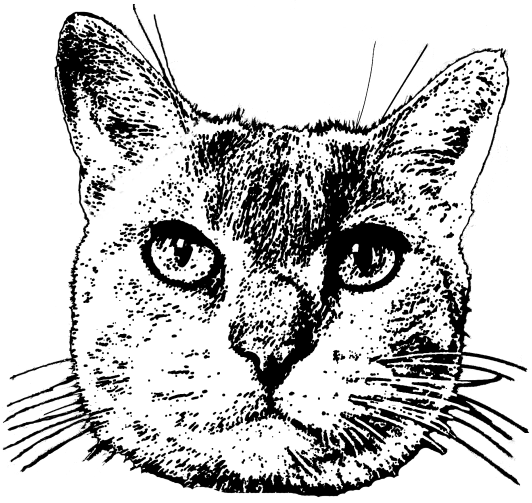
Bevindingenrapport voor Organisatie Rieven

KEIKO 0.0.1.dev1

12 februari 2024



Hoofdstuk 1

Over dit document

1.1 Vertrouwelijkheid

In de informatiebeveiliging wordt gewerkt met het Traffic Light Protocol (TLP). Dit is een internationale uniforme afspraak aan de hand van de kleuren van het verkeerslicht. Het geeft aan hoe vertrouwelijk informatie in het document is en of deze gedeeld mag worden met andere personen of organisaties.

- TLP:RED. Deze informatie heeft de hoogste vertrouwelijkheid. Deze mag niet met andere personen of organisaties worden gedeeld. Vaak zal deze informatie mondeling worden doorgegeven. In veel gevallen ook niet via e-mail of op papier, maar het kan natuurlijk wel.
- TLP:AMBER. Deze informatie mag op een need to know-basis worden gedeeld binnen de eigen organisatie en de klanten (of aangesloten partijen).
- TLP:AMBER+STRICT. Deze informatie mag alleen binnen de eigen organisatie worden gedeeld met mensen voor wie toegang noodzakelijk is. Dit is op een 'need to know'-basis binnen de eigen organisatie.
- TLP:GREEN. Deze informatie is beschikbaar voor iedereen binnen de gemeenschap, waarop ze gericht is. Dat betekent dat het nuttig kan zijn en daarmee gedeeld kan worden op basis van 'nice to know'. Er is geen restrictie tot de eigen organisatie.
- TLP:CLEAR. Deze informatie is niet vertrouwelijk en kan openbaar worden gedeeld.

Dit document is gerubriceerd als TLP:AMBER.

Inhoudsopgave

Hoofdstuk 2

Overzicht

2.1 Samenvatting

Dit zijn de bevindingen van een OpenKAT-analyse op 2024-02-13 23:02:59 UTC. De volgende filters zijn van toepassing op deze bevindingen:

Observed at	2024-02-13
Severities	
Exclude muted	True
Only muted	False

Kopieer deze link om dit rapport te reproduceren.

2.2 Totalen

Niveau	Uniek	Totaal aantal voorvallen
critical	0	0
high	0	0
medium	11	29
low	4	14
recommendation	1	4
pending	0	0
unknown	0	0
Totaal	16	47

2.3 Bevinding types

Risico niveau	Bevindingstype	Voorvallen
medium	KAT-NO-DKIM	1
medium	KAT-NO-DMARC	3
medium	KAT-NO-DNSSEC	10
medium	KAT-NO-SPF	1
medium	RetireJS-jquerymigrate-f3a3	2
medium	RetireJS-jquerymigrate-f901	2
medium	CVE-2016-10735	2
medium	CVE-2018-14040	2
medium	CVE-2018-14041	2
medium	CVE-2018-14042	2
medium	CVE-2019-8331	2
low	KAT-EXPIRED-RPKI	1
low	KAT-INVALID-RPKI	8
low	KAT-NO-RPKI	1
low	KAT-WEBSERVER-NO-IPV6	4
recommendation	KAT-NAMESERVER-NO-IPV6	4

Hoofdstuk 3

Bevindingen

3.1 KAT-NO-DKIM

3.1.1 Bevinding informatie

Bevinding	KAT-NO-DKIM
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	This hostname does not support a DKIM record.
Aanbeveling	Set a DKIM record to protect your domain.

3.1.2 Voorvallen

Hostname | internet | mispo.es

This hostname does not support DKIM records

3.2 KAT-NO-DMARC

3.2.1 Bevinding informatie

Bevinding	KAT-NO-DMARC
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	This hostname does not have a DMARC record.
Aanbeveling	Set a DMARC record to protect your domain.

3.2.2 Voorvallen

Hostname | internet | domaindiscount24.net

This hostname does not have a DMARC record

Hostname | internet | mispo.es

This hostname does not have a DMARC record

Hostname | internet | rieven.com

This hostname does not have a DMARC record

3.3 KAT-NO-DNSSEC

3.3.1 Bevinding informatie

Bevinding	KAT-NO-DNSSEC
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	The provided domain does not have DNSSEC enabled.
Aanbeveling	Enable DNSSEC on your name servers.

3.3.2 Voorvallen

Hostname | internet | domaindiscount24.net

Domain domaindiscount24.net is not signed with DNSSEC.

Hostname | internet | mispo.es

Domain mispo.es is not signed with DNSSEC.

Hostname | internet | ngrane.com

Domain ngrane.com is not signed with DNSSEC.

Hostname | internet | ns1.domaindiscount24.net

Domain ns1.domaindiscount24.net is not signed with DNSSEC.

Hostname | internet | ns1.ngrane.com

Domain ns1.ngrane.com is not signed with DNSSEC.

Hostname | internet | ns2.domaindiscount24.net

Domain ns2.domaindiscount24.net is not signed with DNSSEC.

Hostname | internet | ns2.ngrane.com

Domain ns2.ngrane.com is not signed with DNSSEC.

Hostname | internet | ns3.domaindiscount24.net

Domain ns3.domaindiscount24.net is not signed with DNSSEC.

Hostname | internet | rieven.com

Domain rieven.com is not signed with DNSSEC.

Hostname | internet | www.mispo.es

Domain www.mispo.es is not signed with DNSSEC.

3.4 KAT-NO-SPF

3.4.1 Bevinding informatie

Bevinding	KAT-NO-SPF
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	This hostname does not have an SPF record.
Aanbeveling	Set an SPF record to protect your domain.

3.4.2 Voorvallen

Hostname | internet | mispo.es

This hostname does not have an SPF record

3.5 RetireJS-jquerymigrate-f3a3

3.5.1 Bevinding informatie

Bevinding	RetireJS-jquerymigrate-f3a3
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	cross-site-scripting. More information at: http://blog.jquery.com/2013/05/01/jquery-migrate-1-2-0-released/ or https://github.com/jquery/jquery-migrate/issues/36

3.5.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | jQuery Migrate | 1.0.0 |

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | jQuery Migrate | 1.0.0 |

This JavaScript Library has known vulnerabilities

3.6 RetireJS-jquerymigrate-f901

3.6.1 Bevinding informatie

Bevinding	RetireJS-jquerymigrate-f901
Risico niveau	6.9 / 10
Ernst	Medium
Beschrijving	Selector interpreted as HTML. More information at: http://bugs.jquery.com/ticket/11290 or http://research.insecurelabs.org/jquery/test/

3.6.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | jQuery Migrate | 1.0.0 |

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | jQuery Migrate | 1.0.0 |

This JavaScript Library has known vulnerabilities

3.7 CVE-2016-10735

3.7.1 Bevinding informatie

Bevinding	CVE-2016-10735
Risico niveau	6.1 / 10
Ernst	Medium
Beschrijving	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.
Bron	https://cve.circl.lu/cve/CVE-2016-10735

3.7.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

3.8 CVE-2018-14040

3.8.1 Bevinding informatie

Bevinding	CVE-2018-14040
Risico niveau	6.1 / 10
Ernst	Medium
Beschrijving	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.
Bron	https://cve.circl.lu/cve/CVE-2018-14040

3.8.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

3.9 CVE-2018-14041

3.9.1 Bevinding informatie

Bevinding	CVE-2018-14041
Risico niveau	6.1 / 10
Ernst	Medium
Beschrijving	In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.
Bron	https://cve.circl.lu/cve/CVE-2018-14041

3.9.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

3.10 CVE-2018-14042

3.10.1 Bevinding informatie

Bevinding	CVE-2018-14042
Risico niveau	6.1 / 10
Ernst	Medium
Beschrijving	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.
Bron	https://cve.circl.lu/cve/CVE-2018-14042

3.10.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

3.11 CVE-2019-8331

3.11.1 Bevinding informatie

Bevinding	CVE-2019-8331
Risico niveau	6.1 / 10
Ernst	Medium
Beschrijving	In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Bron	https://cve.circl.lu/cve/CVE-2019-8331

3.11.2 Voorvallen

SoftwareInstance | HostnameHTTPURL | https | internet | mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

SoftwareInstance | HostnameHTTPURL | https | internet | www.mispo.es | 443 | / | Software | Bootstrap | 3.3.7 | cpe:/a:getbootstrap:bootstrap

This JavaScript Library has known vulnerabilities

3.12 KAT-EXPIRED-RPKI

3.12.1 Bevinding informatie

Bevinding	KAT-EXPIRED-RPKI
Risico niveau	3.9 / 10
Ernst	Low
Beschrijving	The route announcement that is matched by the published Route Policy and Authorization (RPKI) is expired
Aanbeveling	Make sure that the Route Origin Authorizations (ROAs) that specify which Autonomous Systems (AS) are authorized to announce your IP addresses are valid and not expired.

3.12.2 Voorvallen

IPAddressV4 | internet | 31.187.70.163

The route announcement that is matched by the published Route Policy and Authorization (RPKI) is expired

3.13 KAT-INVALID-RPKI

3.13.1 Bevinding informatie

Bevinding	KAT-INVALID-RPKI
Risico niveau	3.9 / 10
Ernst	Low

Beschrijving	The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)
Aanbeveling	Make sure that the Route Origin Authorizations (ROAs) that specify which Autonomous Systems (AS) are authorized to announce your IP addresses are valid and not expired.

3.13.2 Voorvallen

IPAddressV4 | internet | 109.234.111.81

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV4 | internet | 134.209.85.72

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV4 | internet | 144.217.35.18

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV4 | internet | 66.206.3.125

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV4 | internet | 94.23.153.36

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV6 | internet | 2001:41d0:c:388:94:23:153:36

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV6 | internet | 2604:4500:c:3:66:206:3:125

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

IPAddressV6 | internet | 2607:5300:60:5e1c:144:217:35:18

The IP address does not have a valid route announcement that is matched by the published Route Policy and Authorization (RPKI)

3.14 KAT-NO-RPKI

3.14.1 Bevinding informatie

Bevinding	KAT-NO-RPKI
Risico niveau	3.9 / 10
Ernst	Low
Beschrijving	The IP address does not have a route announcement that is matched by the published Route Policy and Authorization (RPKI)
Aanbeveling	Work on implementing RPKI for your IP addresses. This may involve creating Route Origin Authorizations (ROAs) that specify which Autonomous Systems (AS) are authorized to announce your IP addresses.

3.14.2 Voorvallen

IPAddressV4 | internet | 31.187.70.163

The IP address does not have a route announcement that is matched by the published Route Policy and Authorization (RPKI)

3.15 KAT-WEBSERVER-NO-IPV6

3.15.1 Bevinding informatie

Bevinding	KAT-WEBSERVER-NO-IPV6
Risico niveau	3.9 / 10
Ernst	Low
Beschrijving	For this website there is no web server with an IPv6 address available.
Aanbeveling	Add an IPv6 address for at least one web server that has no IPv6 address yet.

3.15.2 Voorvallen

Hostname | internet | domaindiscount24.net

There are no webservers with an IPv6 address.

Hostname | internet | mispo.es

There are no webservers with an IPv6 address.

Hostname | internet | ngrane.com

There are no webservers with an IPv6 address.

Hostname | internet | rieven.com

There are no webservers with an IPv6 address.

3.16 KAT-NAMESERVER-NO-IPV6

3.16.1 Bevinding informatie

Bevinding	KAT-NAMESERVER-NO-IPV6
Risico niveau	0.0 / 10
Ernst	Recommendation
Beschrijving	This nameserver does not have an ipv6 address.

3.16.2 Voorvallen

DNSNSRecord | internet | ngrane.com | ns1.ngrane.com.

This nameserver has no ipv6 address

DNSNSRecord | internet | ngrane.com | ns2.ngrane.com.

This nameserver has no ipv6 address

DNSNSRecord | internet | rieven.com | ns1.ngrane.com.

This nameserver has no ipv6 address

DNSNSRecord | internet | rieven.com | ns2.ngrane.com.

This nameserver has no ipv6 address

Hoofdstuk 4

Verklarende Woordenlijst

Begrip	Betekenis
CVSS	Common Vulnerability Scoring System. Systeem om een score te geven aan een zwakke plek in soft - ware. Hoe hoger de score, hoe zwakker de plek. Een organisatie kan deze score gebruiken om te bepalen welke zwakke plekken ze als eerste gaat oplossen. Meer informatie over het scoresysteem staat op hrefhttps://www.first.org/cvss/.
Document	Er zijn in de wetgeving twee definities van een document, die beiden duidelijk maken dat in de juridische zin een document iedere vorm van informatie is, zoals een schriftelijk stuk, e-mail, social media bericht, database, enzovoort. In de Wet op de parlementaire enquete is een document in artikel 1, eerste lid onder c gedefinieerd als Schriftelijk stuk of ander materiaal dat gegevens bevat. In de Wet open overheid is dit in artikel 2, eerste lid gedefinieerd als: document: een door een orgaan, persoon of college als bedoeld in artikel 2.2, eerste lid, opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college;

Begrip	**Betekenis**
Informatiebeveiliging	Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Ontstaat er wel een probleem met de informatie? Dan zorgt informatiebeveiliging ervoor dat de gevolgen zoveel mogelijk beperkt worden.
Risico	Kans op schade of verlies in een computersysteem, gecombineerd met de gevolgen die deze schade heeft voor de organisatie. Een voorbeeld van schade kan bijvoorbeeld zijn dat mensen informatie zien die ze niet hadden mogen zien. Of dat men niet meer zeker weet of gegevens nog kloppen. Bij gevolgen voor de organisatie kan men denken aan financiële schade of het verlies van de goede naam van de organisatie.
TLP	Traffic Light Protocol. Een methode om data of informatie in te delen in klasses. Hoe men dit indeelt, hangt af van met wie men de informatie mag delen. De klasses zijn rood, oranje, groen en wit.
Vertrouwelijkheid	Informatie is vertrouwelijk als het alleen gezien wordt door iemand die het gegeven ook mag zien. Degene die het gegeven maakt, bepaalt wie het mag zien. Vertrouwelijkheid is een van de kwaliteitskenmerken van gegevens.