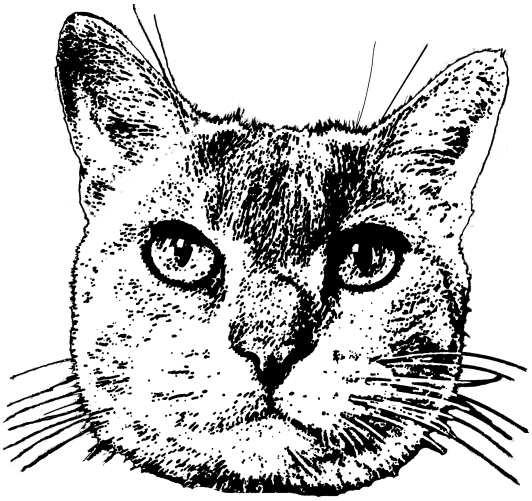
Bevindingenrapport voor Organisatie Rieven

KEIKO 0.0.1.dev1

13 juli 2023



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 2023-07-13 11:07:28 UTC.

2.2 Totalen

Niveau	Uniek	Totaal aantal voorvallen
critical	0	0
high	1	1
medium	1	1
low	0	0
recommendation	0	0
pending	2	3
unknown	0	0
Totaal	4	5

2.3 Bevinding types

Risico niveau	Bevindingstype	Voorvallen
high	CVE-2012-0001	1
medium	CVE-2023-33817	1
pending	KAT-998	1
pending	KAT-999	2

Hoofdstuk 3

Bevindingen

3.1 CVE-2012-0001

3.1.1 Bevinding informatie

Bevinding	CVE-2012-0001
Risico niveau	9.3 / 10
Ernst	High
Beschrijving	The kernel in Microsoft Windows XP SP2, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly load structured exception handling tables, which allows context-dependent attackers to bypass the SafeSEH security feature by leveraging a Visual C++ .NET 2003 application, aka "Windows Kernel SafeSEH Bypass Vulnerability."
Bron	https://cve.circl.lu/cve/CVE-2012-0001

3.1.2 Voorvallen

Network | internet

Test

3.2 CVE-2023-33817

3.2.1 Bevinding informatie

Bevinding	CVE-2023-33817
Risico niveau	8.8 / 10
Ernst	Medium

Beschrijving	hoteldruid v3.0.5 was discovered to contain a SQL injection vulnerability.
Bron	https://cve.circl.lu/cve/CVE-2023-33817

3.2.2 Voorvallen

Network | internet

TEST

3.3 KAT-998

3.3.1 Bevinding informatie

Bevinding	KAT-998
Risico niveau	0.0 / 10
Ernst	Pending

3.3.2 Voorvallen

Network | internet

ja

3.4 KAT-999

3.4.1 Bevinding informatie

Bevinding	KAT-999
Risico niveau	0.0 / 10
Ernst	Pending

3.4.2 Voorvallen

DNSZone | internet | ngrane.com

seee

Network | internet

TEST

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.