

# KPN Security Policy



## KSP – Rule

Title	Technical Vulnerability Management	<pre>graph TD; A[Top level policy (mandatory)] --&gt; B[Standards (mandatory)]; B --&gt; C[Rules (mandatory)]; C --&gt; D[Guidelines (supporting)]; D --&gt; E[Tools (supporting)];</pre>
ID	KSP-FA05-RL03	
Funct. Area	05 - System and Network Security	
Date	5 February 2016	
Version	v2.4	
Status	Approved	
Owner	CISO	

### Summary

Purpose of this document is to set the requirements for a vulnerability management process based on a scan-prioritise-solve cycle in which we continuously check:

- how vulnerable our technical environment is to currently known vulnerabilities
- how our technical environment holds up to best practices
- set priorities based on the scan results and plan fixes or mitigating actions based on that priority.

We consider a vulnerability to be a weakness in a product or configuration, which allows an attacker to reduce a system's information assurance.

Scope for the document is to cover all KPN owned applications, devices or systems connected to an IP network (whether the network is a public one or a KPN one).

### Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

<b>ID</b>	KSP-FA05-RL03-R01
<b>Title</b>	<u>Vulnerability scanning</u>
<b>Description</b>	<p>Every KPN asset connected to a network must be scanned for vulnerabilities at least once per month with a vulnerability scanner. All interfaces of the asset must be scanned; including the logical.</p> <p>N.B.: Customer assets hosted on the KPN network are excluded, as they are not KPN assets.</p>
<b>Relating document</b>	Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)

<b>ID</b>	KSP-FA05-RL03-R02
<b>Title</b>	<u>Centrally managed vulnerability scanning</u>
<b>Description</b>	The vulnerability scanning must be managed centrally for the whole of KPN, not by each segment individually. The owner and thus the segments must take appropriate measures to resolve the reported findings.
<b>Relating document</b>	Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)

ID	KSP-FA05-RL03-R03																
Title	<u>Vulnerability mitigation</u>																
Description	<p>Identified vulnerabilities (whether found based on the monthly vulnerability scanning, or found though other means) must be fixed according to the following timelines:</p> <table><tr><th>Category</th><th>CVSS Score*</th><th>Remediation time in case internet facing</th><th>Remediation time in case not internet facing</th></tr><tr><td>Low</td><td>0,0 - 3,9</td><td>Best effort</td><td>Best effort</td></tr><tr><td>Medium</td><td>4,0 - 6,9</td><td>1 month</td><td>2 months</td></tr><tr><td>High</td><td>7,0 - 10</td><td>2 weeks</td><td>1 month</td></tr></table> <p>If a vulnerability cannot be fixed, mitigating measures must be implemented according to the timeframe.</p> <p>*Common Vulnerability Scoring System (CVSS) Score. Several vendors have their own definition of Low/Medium/High. To not be tied to a specific product or vendor, the categories are based on CVSS Scores. CVSS is a vulnerability scoring system designed by the Forum of Incident Response and Security Teams (FIRST) to provide an open and standardized method for rating IT vulnerabilities and is considered an industry standard for scoring vulnerabilities.</p>	Category	CVSS Score*	Remediation time in case internet facing	Remediation time in case not internet facing	Low	0,0 - 3,9	Best effort	Best effort	Medium	4,0 - 6,9	1 month	2 months	High	7,0 - 10	2 weeks	1 month
Category	CVSS Score*	Remediation time in case internet facing	Remediation time in case not internet facing														
Low	0,0 - 3,9	Best effort	Best effort														
Medium	4,0 - 6,9	1 month	2 months														
High	7,0 - 10	2 weeks	1 month														
Relating document	Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)																