

Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 8:07:55 PM

Selected by: Ruud Leurs

Requirement	Vulnerability scanning
Description	All KPN assets connected to a network, must be scanned for vulnerabilities on a minimum monthly basis. All interfaces, including the logical and external interfaces, must be scanned. The asset owner of the system on which the vulnerabilities have been found must take measures in response to the findings.
Supplement	<p>Customers' assets that are part of the KPN network are not in scope for vulnerability scanning.</p> <p>Vulnerability management on KPN assets with an interface in a black zone, not being Internet or KOEN, may deviate from this rule if other, by CISO approved ways, regular management of vulnerabilities are met.</p>
ID	KSP-RE-253
Version	1.1
Date	November 2, 2018
Rationale	Vulnerability scanning- and management

Requirement	Centrally managed vulnerability scanning
Description	Vulnerability scanning must be managed centrally and managed for the entire KPN organization.
ID	KSP-RE-254
Version	1.1
Date	November 2, 2018
Rationale	Vulnerability scanning- and management

Requirement	Vulnerability mitigation																
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 v2 Base 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>Portal authority findings of CVSS 4.0 or higher need to be solved before go Live. (Portal authority base scores on CVSS v3)</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 v2 Base scores. CVSS v3 in development.</p>	Category	CVSS v2 Base 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 v2 Base 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														
ID	KSP-RE-255																
Version	1.0																
Date	December 11, 2017																
Rationale	Vulnerability scanning- and management																

Requirement	Updates
Description	Security updates must be installed per the timelines set in KSP-RE-255 (Vulnerability mitigation) on all KPN assets. This must be verified regularly. Deviations must be resolved as quickly as possible.
ID	KSP-RE-256
Version	1.0
Date	December 11, 2017
Rationale	Vulnerability scanning- and management

Requirement	Vulnerability management
Description	A vulnerability management process must be implemented and followed.
ID	KSP-RE-257
Version	1.1
Date	November 2, 2018
Rationale	Vulnerability scanning- and management

Requirement	Vulnerability Management
Description	Every system is to be scanned for vulnerabilities on a regular basis. The resulting findings need to be resolved within a pre-defined timeframe depending on the severity.
Supplement	<p>Vulnerabilities can arise over time and must be solved timely to keep the system sufficient safe for attacks.</p> <p>i.e. Schedule of vulnerability tests for systems</p> <p>Isolated systems (without network link and no mobile storage applicable) have no need for vulnerability management.</p>
ID	KSP-RE-258
Version	1.0
Date	December 11, 2017
Rationale	Vulnerability scanning- and management