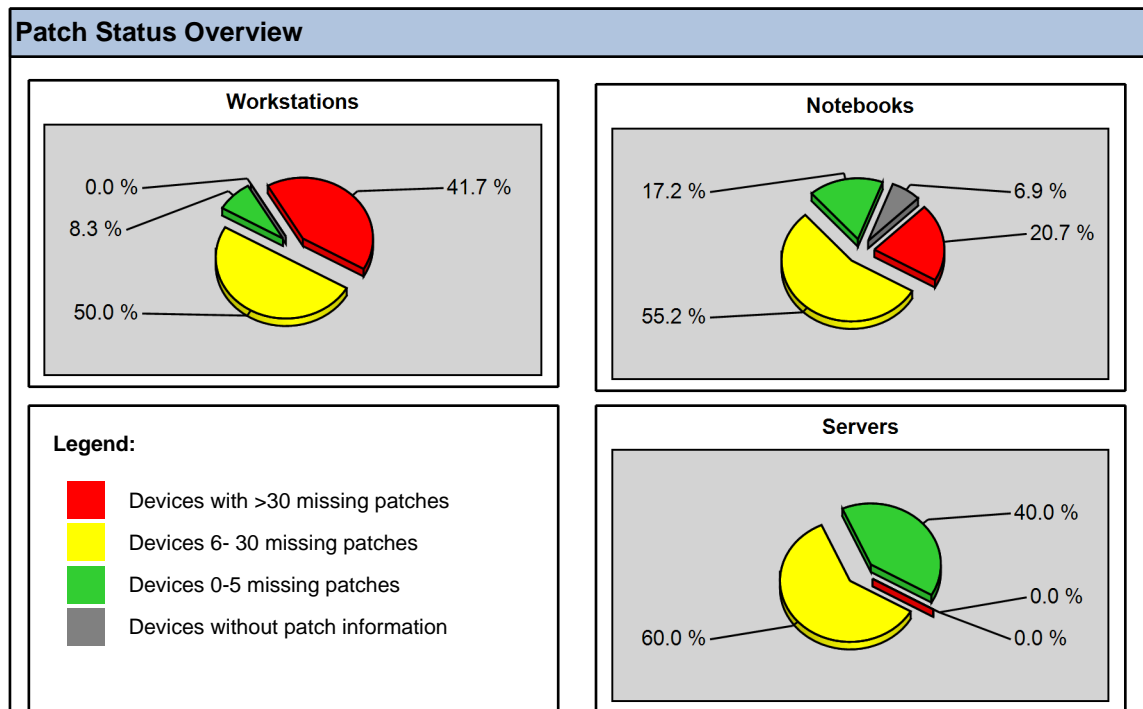


Vulnerability Status Overview:

Vulnerability Status				
	Workstations	Notebooks	Server	
Status calculated on Ø patches missing per device	Critical critical risk for devices to become compromised	High high risk for devices to become compromised	Medium medium risk for devices to become compromised	
Legend:	Ø >30	Ø 16- 30	Ø 6-15	Ø 0-5

Missing Patches			
Devicetype	Missing Patches	Devices	Ø patches missing per device
Workstations	573	12	47
Notebooks	811	29	27
Server	61	6	10
Total	1445	47	30



Patch Status					
Devicetype	Patched	Partial Patched	Unpatched	Unknown	Total
Workstations	1	6	5	0	12
Notebooks	5	16	6	2	29
Server	2	3	0	0	5
Total	8	25	11	2	46

Patch Details:

Missing patches by severity and device types				
Severities	Workstations	Notebooks	Server	Total
Service Packs	13	7	5	25
Critical	315	457	28	800
High	159	184	13	356
Medium	51	101	2	154
Low	4	0	0	4
N/A	0	2	0	2
Unknown	31	60	13	104
Total	573	811	61	1445

Database Statistics:

Known Vulnerability Definitions		Detected Vulnerability Definitions	
Severity	Count	Severity	Count
Service Pack	199	Service Pack	9
Critical	7564	Critical	261
High	641	High	109
Medium	591	Medium	34
Low	702	Low	4
N/A	1011	N/A	2
Unknown	74	Unknown	7
Total	10782	Total	426

Top 10 Vulnerable Devices:

Top 10 Vulnerable Workstations				
Devicename	IP Address	Loginame	Count	Risk status
NDCKYV206	010.006.001.103	IMSMOUSER	134	critical
NDCKYV208	010.006.001.034	ALEXANDERS	114	critical
NDCGBRIMS1	010.000.012.126	FRANKG	109	critical
WFRACP01	010.005.011.023	CPARIS	59	critical
NDCKYV201	010.006.001.120	DMITRYS	56	critical
NDCKYV202	010.006.001.025	DMITRIYT	22	high
NDCGBRIMS	010.000.012.114	NETWORKDIMS	19	high
NDCKYV204	010.006.001.028	VIKTORK	18	high
NDCKYV200	010.006.001.030	JONATHANL	16	high
NDCGBR055	010.000.012.143	MARKM	14	medium

Top 10 Vulnerable Notebooks				
Devicename	IP Address	Loginame	Count	Risk status
NDCGBR031	010.000.012.131	COLLEENM	223	critical
NDCGBR032	010.000.012.116	ANDYF	95	critical
NDCGBR066	010.000.012.102	PHILD	71	critical
NDCMUN100	010.055.017.114	ANDREASN	60	critical
NDCGBR038	010.000.012.145	GERARDG	59	critical
NDCMUN033	010.004.001.102	YVONNES	49	high
NDCMUN650	010.004.001.114	TOBYP	30	high
NETWORKD-LINOR	010.001.001.127	ADMINISTRATOR	29	high
NDCGBR118	010.000.012.108	ANDYF	24	high
NDCMUN036	010.004.001.116	MANUELAG	22	high

Top 10 Vulnerable Server				
Devicename	IP Address	Loginame	Count	Risk status
NDCKYVPDC	010.006.001.009	ADMINISTRATOR	28	high
NDCGBR004	010.000.012.024	FRANKG	15	medium
NDCGBR001	010.000.012.020	ROBERTB	10	medium
NDCGBR002	010.000.012.003	ANDYF	5	low
NDCGBR010	010.000.012.002	FRANKG	3	low

Top 10 Vulnerabilities:

Top 10 Vulnerabilities on Workstations

ID	Title	Language	Severity	Count
FLASHPLAYERv10	Adobe Flash Player ActiveX (version 10.0.22.87)	INTL	Critical	11
LD88-Invoker-20253-882	Client Policy Invoker Fix.	INTL	Critical	6
MS08-074_INTL	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (959070)	INTL	Critical	6
MS09-009_INTL	Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)	INTL	High	6
SKYPEv4.0.0.227	Skype 4.0 (version 4.0.0.227)	INTL	Medium	6
MS08-072_INTL	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (957173)	INTL	Critical	5
MS09-012	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	ENU	High	5
MS09-015	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)	ENU	Medium	5
MS06-022	Vulnerability in ART Image Rendering Could Allow Remote Code Execution (918439)	ENU	Critical	4
MS06-078v2	Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)	ENU	Critical	4

Top 10 Vulnerabilities on Notebooks

ID	Title	Language	Severity	Count
MS09-009_INTL	Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)	INTL	High	19
FLASHPLAYERv10	Adobe Flash Player ActiveX (version 10.0.22.87)	INTL	Critical	14
SKYPEv4.0.0.227	Skype 4.0 (version 4.0.0.227)	INTL	Medium	14
MS09-021_INTL	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	INTL	Critical	12
MS09-027_INTL	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)	INTL	Critical	12
MS08-072_INTL	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (957173)	INTL	Critical	11
MS08-074_INTL	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (959070)	INTL	Critical	11
ADOBERD8v816	Adobe Reader 8.1.6 Update - Multiple Languages	INTL	Critical	9
QTIMEv7.6.2	QuickTime Player (version 7.62.14.0)	INTL	High	9
ITUNESv8.2	iTunes 8.2 (version 8.2.0.23)	INTL	Medium	8

Top 10 Vulnerabilities on Server

ID	Title	Language	Severity	Count
MS07-028	Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)	INTL	Critical	4
MS08-069	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)	ENU	Critical	3
MS06-071	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (928088)	ENU	Critical	2
MS07-042	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)	ENU	Critical	2
MS09-012	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	ENU	High	2
MS09-019	Cumulative Security Update for Internet Explorer (969897)	ENU	Critical	2
MS09-020	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)	ENU	High	2
MS09-022	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	ENU	Critical	2
MS09-025	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)	ENU	High	2

MS09-026	Vulnerability in RPC Could Allow Elevation of Privilege (970238)	ENU	High	2
----------	---------------------------------------------------------------------	-----	------	---