TP Event Details

08/26/2011 3:19 PM

Time	Severity	Filter Num	Name	Protocol
08/23/2011 14:31:52	Critical	1413	1413: Telnet: Sun Solaris Login Bypass (General)	tcp
08/23/2011 14:31:54	Critical	6326	6326: HTTP: Lotus iNotes Buffer Overflow Vulnerability	tcp
08/23/2011 14:31:54	Critical	650	0650: FTP: wu-ftpd File Globbing Heap Corruption	tcp
08/23/2011 14:31:54	Critical	6331	6331: FTP: Novell Netware FTP Buffer Overflow (ZDI-10-062)	tcp
08/23/2011 14:31:54	Low	2232	2232: FTP: 'anonymous' User Login	tcp
08/23/2011 14:31:54	Critical	3476	3476: FTP: NetFTPd Username Overflow	tcp
08/23/2011 14:31:54	Low	6281	6281: FTP: Suspicious Overlong User Command	tcp
08/23/2011 14:31:54	Low	572	0572: DNS: Iquery Attempt (udp)	udp
08/23/2011 14:31:54	Low	6381	6381: MS-RPC: SNA RPC Service Request	tcp
08/23/2011 14:31:54	Low	6381	6381: MS-RPC: SNA RPC Service Request	tcp
08/23/2011 14:31:54	Critical	1698	1698: HTTP: Apache Chunked Encoding Buffer Overflow	tcp
08/23/2011 14:31:54	Critical	3990	3990: Exploit: Shellcode Payload	tcp
08/23/2011 14:31:54	Critical	3766	3766: VERITAS: NetBackup bpjava-msvc Format String Vulnerability (ZDI-05-001)	tcp
08/23/2011 14:31:54	Critical	2292	2292: MS-RPC: DCOM IRemoteActivation Overflow	tcp
08/23/2011 14:31:54	Critical	3602	3602: NDMP: Veritas Backup Exec Client Connect Buffer Overflow	tcp

TP Filter Severity: 'Critical','Major','Minor','Low'; TP Action: 'Permit','Block'; TP Category Names: 'Exploits','Identity Theft','Reconaissance','Security Policy','Spyware','Virus','Vulnerabilities','DDoS','Reputation','Network Equipment Protection','Traffic Normalization','Traffic Thresholds','Peer to Peer','Instant Messaging','Streaming Media'; TP IPS Name: %; TP IPS Names: 'useTextBox'; TP Filter Number: %; TP Filter Name: %; TP VLAN ID: %; TP Source IP: %; TP Destination IP: %; TP SMS IP Address: %; TP Start Event Time: 2011/08/22 00:00:00; TP End Event Tme: 2011/08/26 15:19:17;

TP Category	Action	Hit Count	Profile Name	Source IP	Source Port	Destination IP	Destination Port
Vulnerabilities	Block	1	jphDefault	1.1.166.95	33421	1.2.168.252	23
Vulnerabilities	Block	1	jphDefault	1.3.62.126	12435	1.4.254.98	80
Security Policy	Block	1	jphDefault	1.3.97.32	60428	1.4.220.141	21
Vulnerabilities	Block	1	jphDefault	1.3.207.70	9774	1.4.182.71	21
Security Policy	Block	1	jphDefault	1.3.34.148	3171	1.4.39.170	21
Exploits	Block	1	jphDefault	1.3.54.97	55209	1.4.143.224	21
Security Policy	Block	1	jphDefault	1.3.99.154	8542	1.4.104.212	21
Security Policy	Block	1	jphDefault	1.3.193.136	4878	1.4.121.235	53
Security Policy	Block	1	jphDefault	1.3.65.138	18611	1.4.70.100	1094
Security Policy	Block	1	jphDefault	1.3.71.189	1646	1.4.230.172	1094
Exploits	Block	1	jphDefault	1.3.59.91	8182	1.4.64.157	80
Exploits	Block	1	jphDefault	1.3.116.79	26753	1.4.200.62	2103
Vulnerabilities	Block	1	jphDefault	1.3.126.151	3636	1.4.3.34	13722
Vulnerabilities	Block	1	jphDefault	1.3.80.217	24421	1.4.226.87	135
Vulnerabilities	Block	1	jphDefault	1.3.173.164	51454	1.4.30.0	10000

VLAN ID	SMS IP	IPS Name	Segment	Phy	Trace	Event Id
3050	172.16.212.100	CTL-660n-2	7A 7B	14	0	2527802
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527850
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527849
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527848
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527847
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527846
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527845
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527844
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527843
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527842
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527841
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527840
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527839
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527838
3051	172.16.212.100	CTL2500N-1	6B 6A	11	0	2527837