Top threats

PA-3060-A : Monday, February 27, 2023

Threat/Content Name	ID	Threat/Content Type	Count
HTTP Directory Traversal Vulnerability	54701	vulnerability	3.04 k
HTTP Directory Traversal Request Attempt	30844	vulnerability	2.60 k
Apache Shiro Improper Authentication Vulnerability	58132	vulnerability	1.33 k
Generic HTTP Cross Site Scripting Attempt	31477	vulnerability	858
Apache HTTP Server Path Traversal Vulnerability	91752	vulnerability	723
ENV File Scanning Attempt	93397	vulnerability	624
HTTP SQL Injection Attempt	54608	vulnerability	603
HTTP Directory Traversal Request Attempt	33194	vulnerability	577
Oracle GlassFish Server Directory Traversal Vulnerability	92324	vulnerability	554
HTTP /etc/passwd Access Attempt	35107	vulnerability	457
Microsoft Windows win.ini Access Attempt Detected	30851	vulnerability	344
HTTP SQL Injection Attempt	58209	vulnerability	343
UDP Flood	8502	flood	308
SSH User Authentication Brute Force Attempt	40015	vulnerability	266
HTTP SQL Injection Attempt	38402	vulnerability	262
Apache Struts2 Dynamic Method Remote Code Execution Vulnerability	54739	vulnerability	227
Zimbra Collaboration Memcached CRLF Injection Vulnerability	93011	vulnerability	189
TCP Fast Open	8725	packet	187
Apache Shiro Improper Authentication Vulnerability	58590	vulnerability	183
SFTP Config JSON File Download Attempt	59965	vulnerability	157
Apache Struts2 OGNL Expression Handling Script Injection Vulnerability	34933	vulnerability	138
TCP SYN with data	8723	packet	136
HTTP Cross-Site Scripting Vulnerability	35284	vulnerability	132
HTTP Unauthorized Brute Force Attack	40031	vulnerability	110
Possible HTTP Malicious Payload Detection	58461	vulnerability	108
Apache Log4j Remote Code Execution Vulnerability	91991	vulnerability	106
HTTP /etc/passwd Access Attempt	30852	vulnerability	99
Apache Struts2 Redirect/Action Method Remote Code Execution Vulnerability	56944	vulnerability	86
HTTP Cross Site Scripting Attempt	32658	vulnerability	84
HTTP SQL Injection Attempt	36239	vulnerability	78
Non-RFC Compliant SSL Traffic on Port 443	56112	vulnerability	76
Cisco RV320/RV325 Router Unauthenticated Configuration Export Vulnerability	55025	vulnerability	64
Novell ZENworks Mobile Management Cross-Site Scripting Vulnerability	39766	vulnerability	64
Generic HTTP Cross Site Scripting Attempt	31476	vulnerability	62
rConfig Remote Code Execution Vulnerability	56889	vulnerability	58
HTTP Cross-Site Scripting Vulnerability	57176	vulnerability	52
ZGrab Application Layer Scanner Detection	57955	vulnerability	47
WordPress Easy Digital Downloads Plugin SQL Injection Vulnerability	93401	vulnerability	44
HTTP SQL Injection Attempt	59128	vulnerability	38
Nazgul Nostromo nhttpd Directory Traversal Vulnerability	56937	vulnerability	36
HTTP SQL Injection Attempt	30514	vulnerability	36
Non-RFC Compliant SMTP Traffic on Port 25	56586	vulnerability	35
Possible HTTP Malicious Payload Detection	58463	vulnerability	35
572876837	572876837	spyware	28
Apache Struts Content-Type Remote Code Execution Vulnerability	33196	vulnerability	28
Sonatype Nexus Repository Manager Remote Code Execution Vulnerability	55155	vulnerability	28
Confluence Server OGNL Injection Remote Code Execution Vulnerability	91594	vulnerability	27
HTTP SQL Injection Attempt	35823	vulnerability	26
Apache Struts2 OGNL Remote Code Execution Vulnerability	54691	vulnerability	23
HTTP SQL Injection Attempt	58005	vulnerability	23

paloalto NETWORKS®