Top threats

PA-3060-A : Monday, February 13, 2023

Threat/Content Name	ID	Threat/Content Type	Count
Session Limit Event	8801	flood	7.50 k
HTTP Directory Traversal Vulnerability	54701	vulnerability	2.84 k
HTTP Directory Traversal Request Attempt	30844	vulnerability	2.26 k
Apache HTTP Server Path Traversal Vulnerability	91752	vulnerability	833
Apache Shiro Improper Authentication Vulnerability	58132	vulnerability	733
HTTP Directory Traversal Request Attempt	33194	vulnerability	701
Oracle GlassFish Server Directory Traversal Vulnerability	92324	vulnerability	625
ENV File Scanning Attempt	93397	vulnerability	378
Generic HTTP Cross Site Scripting Attempt	31477	vulnerability	292
TCP Fast Open	8725	packet	271
HTTP SQL Injection Attempt	54608	vulnerability	250
UDP Flood	8502	flood	219
Apache Shiro Improper Authentication Vulnerability	58590	vulnerability	218
SSH User Authentication Brute Force Attempt	40015	vulnerability	193
Zimbra Collaboration Memcached CRLF Injection Vulnerability	93011	vulnerability	166
SFTP Config JSON File Download Attempt	59965	vulnerability	147
Atlassian Jira Server-Side Request Forgery Vulnerability	56606	vulnerability	138
Apache Log4j Remote Code Execution Vulnerability	91991	vulnerability	132
TCP SYN with data	8723	packet	126
Possible HTTP Malicious Payload Detection	58461	vulnerability	122
Microsoft Windows win.ini Access Attempt Detected	30851	vulnerability	100
HTTP Unauthorized Brute Force Attack	40031	vulnerability	85
HTTP SQL Injection Attempt	36241	vulnerability	78
HTTP /etc/passwd Access Attempt	35107	vulnerability	72
Possible HTTP Malicious Payload Detection	58561	vulnerability	72
ZGrab Application Layer Scanner Detection	57955	vulnerability	63
HTTP SQL Injection Attempt	30514	vulnerability	60
HTTP SQL Injection Attempt	93022	vulnerability	50
Apache Web Server Access Control Bypass Vulnerability	54785	vulnerability	49
Zeroshell Remote Command Execution Vulnerability	58706	vulnerability	47
Spring Cloud Config Server Directory Traversal Vulnerability	55558	vulnerability	44
Apache Struts2 Redirect/Action Method Remote Code Execution Vulnerability	56944	vulnerability	44
WordPress Authentication Bypass Vulnerability	93262	vulnerability	43
HTTP /etc/passwd Access Attempt	30852	vulnerability	40
HTTP SQL Injection Attempt	58005	vulnerability	39
HTTP SQL Injection Attempt	35823	vulnerability	38
phf Remote Command Execution Vulnerability	32790	vulnerability	38
Possible HTTP Malicious Payload Detection	58463	vulnerability	37
Linear eMerge E3 Unauthenticated Command Injection Remote Root Exploit Vulnerability	56996	vulnerability	36
Hongdian H8922 Industrial Router Remote Command Execution Vulnerability	91172	vulnerability	36
HTTP SQL Injection Attempt	36239	vulnerability	35
KR Web PHP Remote File Include Vulnerability	91655	vulnerability	32
MVPower DVR Shell Unauthenticated Command Execution Vulnerability	57566	vulnerability	29
Confluence Server OGNL Injection Remote Code Execution Vulnerability	91594	vulnerability	27
Non-RFC Compliant SSL Traffic on Port 443	56112	vulnerability	26
Weaver OA9 Arbitrary File Upload Vulnerability	91188	vulnerability	25
HTTP: User Authentication Brute Force Attempt	40006	vulnerability	25
HTTP SQL Injection Attempt	91515	vulnerability	24
TCP SYN-ACK with data	8724	packet	22
HTTP WWW-Authentication Failed	31708	vulnerability	22