Top threats

PA-3060-A : Thursday, October 13, 2022

Threat/Content Name	ID	Threat/Content Type	Count
Session Limit Event	8801	flood	904.07 k
HTTP SQL Injection Attempt	58209	vulnerability	524.46 k
HTTP SQL Injection Attempt	54608	vulnerability	468.24 k
Fuzz Faster U Fool Tool Detection	90304	vulnerability	451.81 k
UDP Flood	8502	flood	430.93 k
HTTP SQL Injection Attempt	38402	vulnerability	305.13 k
HTTP Directory Traversal Request Attempt	30844	vulnerability	122.07 k
Generic HTTP Cross Site Scripting Attempt	31477	vulnerability	68.78 k
HTTP Unauthorized Brute Force Attack	40031	vulnerability	43.38 k
HTTP Directory Traversal Vulnerability	54701	vulnerability	40.17 k
HTTP /etc/passwd Access Attempt	35107	vulnerability	34.14 k
Microsoft Windows win.ini Access Attempt Detected	30851	vulnerability	22.74 k
HTTP: User Authentication Brute Force Attempt	40006	vulnerability	21.55 k
HTTP SQL Injection Attempt	36239	vulnerability	18.40 k
HTTP SQL Injection Attempt	36056	vulnerability	10.65 k
Novell ZENworks Mobile Management Cross-Site Scripting Vulnerability	39766	vulnerability	9.56 k
PHP Remote File Include Vulnerability	33327	vulnerability	8.87 k
HTTP Cross-Site Scripting Vulnerability	57176	vulnerability	6.79 k
Apache Log4j Remote Code Execution Vulnerability	91991	vulnerability	6.30 k
Confluence Server OGNL Injection Remote Code Execution Vulnerability	91594	vulnerability	6.29 k
HTTP Cross-Site Scripting Vulnerability	35284	vulnerability	6.18 k
HTTP SQL Injection Attempt	30514	vulnerability	5.95 k
HTTP Cross Site Scripting Attempt	32658	vulnerability	5.85 k
HTTP /etc/passwd Access Attempt	30852	vulnerability	3.91 k
Apache Shiro Improper Authentication Vulnerability	58132	vulnerability	3.75 k
Potential FastJson Deserialization Detection	92713	vulnerability	3.70 k
Generic HTTP Cross Site Scripting Attempt	31476	vulnerability	3.19 k
Bash Remote Code Execution Vulnerability	36729	vulnerability	3.05 k
F5 Traffic Management User Interface Remote Code Execution Vulnerability	58623	vulnerability	2.95 k
Apache HTTP Server Path Traversal Vulnerability	91752	vulnerability	2.32 k
Possible HTTP Malicious Payload Detection	58098	vulnerability	2.30 k
Suspicious File Downloading Detection	54469	vulnerability	2.21 k
Cisco ASA and FTD Arbitrary File Read Vulnerability	59021	vulnerability	2.19 k
Apache Log4j Remote Code Execution Vulnerability	92001	vulnerability	2.15 k
Apache Struts2 Remote Code Execution Vulnerability	38040	vulnerability	2.14 k
Car Rental Management System File Inclusion Vulnerability	90136	vulnerability	1.94 k
Microsoft Exchange Server SSRF Vulnerability	91368	vulnerability	1.92 k
HTTP SQL Injection Attempt	58005	vulnerability	1.82 k
HTTP Cross Site Scripting Vulnerability	35864	vulnerability	1.72 k
HTTP Request Directory Path Traversal Detection	90793	vulnerability	1.71 k
Zeroshell Remote Command Execution Vulnerability	58706	vulnerability	1.71 k
Oracle GlassFish Server Directory Traversal Vulnerability	92324	vulnerability	1.70 k
Apache Struts2 OGNL Expression Handling Script Injection Vulnerability	34933	vulnerability	1.66 k
Acunetix Web Vulnerability Scanner Detection	36263	vulnerability	1.54 k
Spring Cloud Gateway Code Injection Vulnerability	92311	vulnerability	1.54 k
Microhard Systems 4G Cellular Ethernet and Serial Gateway Information Disclosure Vulnerability	59127	vulnerability	1.44 k
rConfig Remote Code Execution Vulnerability	56889	vulnerability	1.43 k
Apache Struts2 Dynamic Method Invocation Remote Code Execution Vulnerability	38521	vulnerability	1.42 k
Possible HTTP Malicious Payload Detection	58461	vulnerability	1.29 k
YAWS Unauthenticated Remote File Disclosure Vulnerability	58618	vulnerability	1.22 k