OUTBREAK ALERTS

ABB TotalFlow Path Traversal Vulnerability

High risk vulnerability affecting oil and gas companies

https://library.e.abb.com/public/b17396142a3d4d14ae29e351ccc974ec/Cyber%20Security%20Advisory%20CVE-2022-0902%20-%20Path%20Traversal%20Vulnerability%20in%20Totalflow%20TCP%20protocol.pdf CVEs: CVE-2022-0902

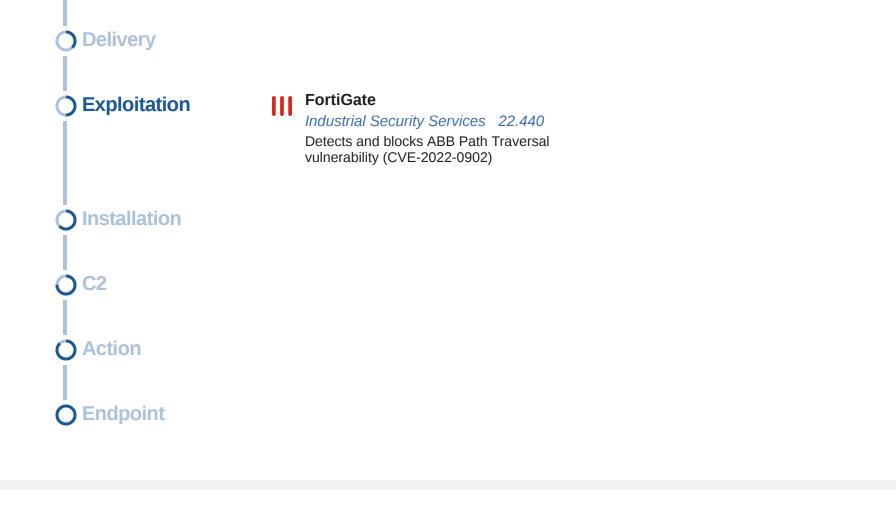
Asea Brown Boveri (ABB), a Swiss industrial automation firm which develops flow computers, a special-purpose electronic instrument used by oil and gas manufacturers to interpret data and calculate oil and gas flow rates and volume are affected by a vulnerability that could allow hackers to cause disruptions and prevent utilities from billing their customers.

Background	A related cyber security incident happened in May 2021, where Colonial Pipeline suffered major disruptions and had to be shut down due to a ransomware attack affecting its billing systems. Any similar attacks can have huge ramifications on operational technologies and poses greater risks to critical supply chains.
Announced	July 14, 2022: ABB posted a security advisory at https://library.e.abb.com/public/b17396142a3d4d14ae29e351ccc974ec/Cyber%20Security%20Advisory%20CVE-2022- 0902%20-%20Path%20Traversal%20Vulnerability%20in%20Totalflow%20TCP%20protocol.pdf
Latest Developments	November 8th, 2022: Claroty posted a detailed research on a path-traversal vulnerability in ABB TotalFlow flow computers and controllers and how an attacker could exploit this vulnerability to inject and execute arbitrary code. https://claroty.com/team82/research/an-oil-and-gas-weak-spot-flow-computers

Cyber Kill Chain

O Reconnaissance

O Weaponization



Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiAnalyzer	Outbreak Detection Version 1.00075 https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00075
	Threat Hunting Version 7.0+ https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-TotalFlow-Path/ta-p/229954
FortiSIEM	<i>Content Update</i> Version 308 https://help.fortinet.com/fsiem/6-6-2/Online-Help/HTML5_Help/content_updates.htm#Content12
	Threat Hunting Version 6.6.0+ https://community.fortinet.com/t5/FortiSIEM/Technical-Tip-Using-FortiSIEM-Content-Updates-to-detect/ta-p/232371
Additional Resources	
NIST	https://nvd.nist.gov/vuln/detail/CVE-2022-0902
Security Week	https://www.securityweek.com/abb-oil-and-gas-flow-computer-hack-can-prevent-utilities-billing-customers
The Hacker News	https://thehackernews.com/2022/11/high-severity-flaw-reported-in-critical.html

Claroty Research

https://claroty.com/team82/research/an-oil-and-gas-weak-spot-flow-computers

Threat Signal

https://www.fortiguard.com/threat-signal-report/4878

