

Reported by: Derick Naraine

Incident Description

Time of First Attack: 12:40:00 PM Time of Attack Detection: 12:00:00 PM  
Estimated Recovery Time: 00:00 Duration of Attack: 00:00  
Has the Attack Ended?: Yes Estimated Damage Account: $0  
Number of Hosts Affected: 0 Number of Users Affected: 0  
Severity of Attack: Low Attack Category: ICS/HMI  
Type of Incident: Active Reconnaissance  
How Did You Become Initially Aware of the Attack?  
Port scan

Impact of Attack

Primary Purpose of Host: HMI/ICS System  
Host Name: HELIOS-HMI IP Address: 10.0.4.10  
Operating System: Ubuntu 16.04  
Applications Affected: SSH

Data Loss/Compromise

Was there any loss or compromise of sensitive data?:  
None.  
Was there any change to the afflicted system?:  
None.  
Was the HMI/ICS affected?:  
No  
Corrective measures enacted:  
Disabled ports