

Reported by: Vincent Monteleone

Incident Description

Time of First Attack: 9:34:00 AM Time of Attack Detection: 10:15:00 AM  
Estimated Recovery Time: 00:44 Duration of Attack: 00:10  
Has the Attack Ended?: Yes Estimated Damage Account: A lot of damage  
Number of Hosts Affected: 10 Number of Users Affected: 15  
Severity of Attack: Elevated Attack Category: Web Server  
Type of Incident: Denial of Service  
How Did You Become Initially Aware of the Attack?  
My mom told me!

Impact of Attack

Primary Purpose of Host: Web Server  
Host Name: HELIOS-WEB IP Address: 10.0.4.7  
Operating System: CentOS 7  
Applications Affected: RDP

Data Loss/Compromise

Was there any loss or compromise of sensitive data?:  
A ton of loss to all data.  
Was there any change to the afflicted system?:  
None  
Was the HMI/ICS affected?:  
Yes  
Corrective measures enacted:  
I made Derick get me coffee.