**UMBC Team 7**
**Status Report**
**Captain: Christian Beam**
**4/1/2017**

# Operational Status

Green = Functional
Yellow = Partially Functional
Red = Not Functional

## **Application Development Server** (KAA)

Status: The development server is fully functional and showed no signs of compromise. We detected multiple attempted intrusions and suspicious login attempts, however none were successful.

Immediate Solution: Continue to monitor the service and fix any discovered security vulnerabilities.

Long-Term Solution: Look into alternatives for inherently secure IoT development.

## **Continuous Integration Server** (Jenkins)

Status: Was subject to a denial of service attack, which we mitigated within 15 minutes. We were able to provide information that led to law enforcement arresting the perpetrator. However, it is currently configured insecurely and Jenkins users have too much power.

Immediate Solution: Reduce operating system level permissions available to Jenkins users to increase security, while preserving functionality.

Long-Term Solution: Replace the service with a more modern Continuous Integration product with better security, such as Drone.

## **Code Repository** (GitLab)

Status: We audited the GitLab configuration for security issues and resolved them within the first hour. Aside from a few weak passwords, no other security issues have been found.

Immediate Solution: Continue to monitor the service and fix any discovered security vulnerabilities.

Long-Term Solution: Upgrade to the enterprise version of GitLab, and configure it to authenticate against our Active Directory. This version of GitLab will also provide a better solution for backing up the server.

## **Data Storage and Visualization Server** (ELK)

Status: We have now configured ELK to allow us to centrally view our logs and correlate malicious traffic.

Immediate Solution: Monitor the incoming data and act proactively to mitigate any problems.

Long-Term Solution: ELK lacks flexible authorization controls. We recommend that we look at implementing the paid X-Pack add-on or migrating to a competitor such as Splunk in the next few weeks.

## **Firewall** (pfSense)

Status: We were able to effectively leverage the firewall to mitigate Denial of Service (DoS) attempts as well as repel and suppress intrusions.

Immediate Solution: We will continue to monitor activity on the network, and change it appropriately when other services require it.

Long-Term Solution: Implement infrastructure monitoring software, such as Nagios to further increase availability. We should consider upgrading to the Palo Alto VM300 series, which will offer additional features to enable us to secure a growing company.

## **Internal Webserver** (Windows XP IIS)

Status: We are mitigating an ongoing, persistent, active attack, however service has been maintained.

Immediate Solution: Isolate XP from the rest of the servers on the network to reduce the impact of compromises. Further investigate attack, and attempt to remove any unauthorized perpetrators.

Long-Term Solution: Windows XP is not currently supported as of April 8, 2014. It is recommended to upgrade the service to be deployed on a Windows Server 2012 R2 or 2016.

## **External Webserver** (Windows 2012 IIS)

Status: This webserver is fully functional and ready to host the external website. There were some intrusions but they have been removed and mitigated. The server is still at risk due to its connections to other machines that are infected.

Immediate Solution: Work to isolate the server from the rest of the network as much as possible without interruption of service.

Long-Term Solution: Maintain current Windows updates. We recommend updating to Windows Server 2016.

## **Webserver Database** (Windows 2003 MSSQL)

Status: We are mitigating an ongoing, persistent, active attack. We have identified and removed one piece of malware. Our service availability has been maintained.

Immediate Solution: Continue close monitoring of the server to sustain the integrity of the database.

Long-Term Solution: Windows 2003 is not currently supported as of July 14, 2015. It is recommended to upgrade to a currently supported windows server such as Windows Server 2012 R2 or Windows Server 2016.

## **Active Directory** (Windows 2008 AD)

Status: AD is up and available, however the adversary is exercising a significant amount of control, and it's proving difficult to remove them.

Immediate Solution: Take the server offline for forensics and reconstruction of the Active Directory.

Long-Term Solution: We recommend upgrading to Windows Server 2016 with current updates to take full advantage of newer security features.

## **Exchange Email Server** (Windows 2008)

Status: The mail service is up and functional, however given its interdependencies with Active Directory, the adversary has undoubtedly achieved a partial compromise.

Immediate Solution: Re-securing Active Directory is the first priority, followed by hardening of the host and sweeping for any persistence mechanisms.

Long-Term Solution: We recommend upgrading to Windows Server 2016 with current updates to take full advantage of newer security features. We also recommend upgrading to the 2016 version of exchange.

## **Application Deployment and Security** (Windows 2012 SCCM)

Status: The web server is operational. However given SCCM's tightly coupled integration with Active Directory, it cannot be considered completely set up. We patched a remote code execution vulnerability in IIS, the host has been secured and the adversary's persistence has been removed.

Immediate Solution: We will prevent re-exploitation through patching and firewalling.

Long-Term Solution: Apply all applicable Windows patches, not just critical actively exploited ones.