McAfee Professional Services

Unisys ClearPath OS 2200 Security Assessment White Paper

Prepared for Unisys Corporation
April 25, 2017
Table of Contents

Executive Summary .......................................................................................................................... 3
ClearPath Forward OS 2200 Summary .......................................................................................... 3
Testing Rationale & Methodology ................................................................................................. 4
  Threat Modeling .......................................................................................................................... 4
  OS 2200 Penetration Testing & Security Configuration Review ............................................... 4
  Apex Management Web Application & Apex Agent Penetration Testing .............................. 5
  Network Protocol Analysis and Fuzz Testing ......................................................................... 6
  File Based Fuzz Testing ........................................................................................................ 7
Areas of Analysis & Recommendation ...................................................................................... 7
Conclusions .................................................................................................................................... 11
About McAfee ............................................................................................................................... 12
About McAfee Professional Services ............................................................................................ 12
Executive Summary
Unisys coordinated with Foundstone Services, part of the McAfee Professional Services offering, on a multiphase independent product security assessment against the Unisys ClearPath OS 2200 (OS 2200) enterprise-class operating system. At the conclusion of the assessment, Foundstone rated both the OS 2200 operating system and the Apex administrative software as highly secure. The scope of this project focused on the OS 2200 core operating system and management interface security. The test environment used consisted of both the ClearPath Software Series OS 2200 Developer Studio and a Dorado 8480 Server, configured to Security Level 1.

The engagement consisted of a threat modelling exercise, an operating system evaluation, a detailed assessment of the management interfaces, penetration testing and a configuration assessment.

Foundstone consultants conducted a security review and exploitative penetration testing, from the perspective of differing threat actors, operating on the enterprise LAN inside the perimeter firewalls, during phases 2 and 3 of the assessment. The original testing began in January 2017 with retesting conducted in March 2017. Foundstone consultants provided daily feedback to the Unisys team to discuss findings, work with the development and architecture teams on remediation and determine root cause.

This document provides a security overview of OS 2200, based on the white box security testing conducted by Foundstone. The OS 2200 operating system was designed for an enterprise class client base, requiring a high level of information security and assurance, and an operating system designed to exceed information security best practices for authorization, resource management, and reliability.

During the security assessment, attacks using both basic and sophisticated techniques failed to compromise data security and integrity, and denial of service attacks were successfully remediated. Foundstone identified recommendations for enhancing OS 2200 and the administrative interface Apex. Unisys addressed the recommendations and Foundstone verified the changes. Unisys has made them available in software updates for clients using both the tested system level (Release 17) and the previous one (Release 16).

ClearPath Forward OS 2200 Summary
The Unisys ClearPath Forward OS 2200 operating system is designed to provide a robust and secure platform for a wide variety of customer requirements. Therefore the security requirements for an OS 2200 system are highly specific to each customer’s application and security requirements.

In recognition and as a response to these diverse customer requirements, Unisys has developed the concept of Security Levels. These are a set of OS 2200 security configuration
templates, designed to support a broad range of customer information security objectives. Fundamental security and security levels 1 through 3 each provide sets of capabilities that a client can enable. Increasing the security level provides a more rigidly protected OS 2200 environment for sites with more stringent information security requirements.

The operating system kernel of OS 2200 provides a fine grained security mechanism based on the principle of least privilege. This principle demands that only the minimum privilege be granted necessary to perform the task required. Therefore, the OS 2200 operating system has no concept of a super user role, unlike most other operating systems, which can be assumed by any user. Rather OS 2200 uses a large set of specific privileges which may be granted separately to each user, each privilege being associated with a specific authority. The OS 2200 Exec contains all the code in the system allowed to run at the highest privilege levels. There are no mechanisms for other code to be promoted to those privilege levels. The Exec is responsible for managing the system hardware, scheduling and managing work, and communicating with operators and administrators. The OS 2200 Exec is central to the real time, multi-threaded interactive, transaction and batch processing system. OS 2200 implements a fully virtual file system. The files may be allocated anywhere across any of the mass storage devices.

**Testing Rationale & Methodology**

**Threat Modeling**

The threat-modeling process began with a high-level architecture review of the OS 2200 operating system's design in order to understand the overall platform's functionality, security considerations and deployment scenarios. Foundstone consultants worked with the Unisys architects and development teams to understand the implementation of the security controls within the operating system and applications.

Through meetings, Q & A “round tables” and a thorough review of the detailed documentation provided by Unisys, Foundstone consultants derived a list of credible threats to the various components that make up the solution. This process resulted in a number of test scenarios relating to the OS 2200 test bed and its attack surface and a profile for the potential threat actors within these scenarios. This work was then used to inform the testing approach, the methodology used, and the threat actor selection, used during the following phases of the engagement for Unisys.

**OS 2200 Penetration Testing & Security Configuration Review**

The Internal Penetration Testing against the OS 2200 environment sought to attack the operating systems from the perspective of both an authenticated network-based user and an unauthenticated network-based user. Testing concentrated on the services advertised and the possibility of vulnerabilities in these services that could be leveraged by an attacker, to compromise the integrity of the systems and the data stored, processed, and transmitted by them.
In addition a Security Configuration Review was performed to assess the effectiveness of the security controls applied by an OS 2200 instance configured at Security Level 1. The systems reviewed during this engagement were configured in accordance with publicly available documentation provided by Unisys. The tests conducted sought to enumerate, analyze, test and evidence the presence and effectiveness of the Security Level 1 OS 2200 security controls, across the operating system.

These controls are core to the maintenance of the confidentiality, integrity and availability of assets stored, processed and transmitted by the operating system.

The System Security Review was performed using both interview-based questioning of the development team, application specialists, security consultant and operational team and an interactive review of the settings on the test systems provided. This approach provided an effective means of rapidly determining the nature of the configured host-based security controls.

**Apex Management Web Application & Apex Agent Penetration Testing**

Following the Threat Assessment of the OS 2200 architecture and its operating environments, it was determined that the Apex Web Management interface and Apex Agent should be comprehensively assessed. The penetration test against the Apex web application (external to OS 2200) and Apex Agent (OS 2200 resident) was governed by industry-recognized testing methodologies to provide a thorough review of the web management components, the servers on which they reside and the code base responsible for their effective operation. The testing began with network, operating system, and web server level scans to search for known vulnerabilities and common misconfigurations.

Foundstone consultants then performed an application discovery process to gather information about the Apex web application. With this data, Foundstone then conducted more detailed testing, which consisted of input validation tests, impersonation (authentication and authorization) tests, and session state management checks.

The Apex web management interface is presented as an ASP.NET web application on a Microsoft IIS 8.5 web server. The Apex application is recommended by Unisys as an internally exposed management interface for the configuration of the OS 2200 operating system. Apex consolidates administrative tasks that have traditionally been performed by other products using other communication protocols such as INT1 (a Unisys proprietary protocol) and SNMP. The Apex web application communicates directly with the Apex Agent service on the OS 2200 via encrypted web sockets in the test environment. The high-level Apex architecture is represented below:
Figure 1: Apex Architecture

Network Protocol Analysis and Fuzz Testing

Within the ClearPath Forward OS 2200 test environment, several proprietary network protocols and protocol implementations were tested. Testing was performed against these protocols as both an unauthenticated user with network level access to the exposed interface and as an authenticated network user.

The INT1 protocol is a Unisys proprietary command protocol similar to telnet that can be configured on OS 2200 systems for user interaction and systems management activity. Therefore, being able to analyze and understanding this protocol, dissect it effectively and monitor the communications between the client and the OS 2200 hosts, were critical attack activities to perform to provide a more complete set of security assurances for OS 2200.

In addition to INT1 there are several protocols supported by OS 2200 that adhere to open standards. The Foundstone Consultants analyzed these protocols and replicated them using custom fuzz scripts, designed to fuzz the OS 2200 protocol implementations. These target protocols included SNMP, FTP, WebSocket (Apex agent) and CIFS.
File Based Fuzz Testing

Following a Threat Assessment, File Format Fuzzing was used to simulate one of a range of malicious activities which could be performed by a malicious, authenticated and privileged OS 2200 user. File format fuzzing is a testing strategy designed to find bugs in native OS 2200 software, installed on the systems under test conditions. The approach used a sample file of 15k bytes and a large number of test cases were generated with malformed file components to target the OS 2200 software subject. Scripts were generated to open the test cases and monitor the application and system responses.

File format fuzz testing focused on the ZIPUT utility. This is the standard zip compression utility for the OS 2200 environment. From the 15kb .zip sample file, approximately 8000 test cases were generated, with varying ratios and formats of fuzz data.

Areas of Analysis & Recommendation

<table>
<thead>
<tr>
<th>Analysis Topic</th>
<th>Best Practice</th>
<th>Evaluation</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level 1 Configuration Assessment</td>
<td>Apply stringent resource restrictions based on user access requirements. Vendors should encourage secure installations of products. Optional security settings should be configured in the default secure state.</td>
<td>OS 2200 allows administrators to configure OS 2200 to select a comprehensive set of security control configurations to meet a specific organisation's security objectives. In addition to the templated Security Levels to govern the OS 2200 system security settings, Unisys has published a security support library allowing customers to customize the operating system's security controls to meet their specific requirements. The evaluation of the Security Level 1 systems performed by Foundstone was conducted through interactive systems testing, interview-led questioning with the</td>
<td>Clients should follow the comprehensive documentation guides and recommendations provided by Unisys when building and configuring their OS 2200 environment. These guides provide a well-structured recommended configuration and options for tailoring customers' OS 2200 systems, for specific operational security goals. During testing the controls implemented and configured at Security Level 1 proved resilient to attack and circumvention. Foundstone was unable to circumvent or undermine the effectiveness of the operating systems controls configured at Security Level 1.</td>
</tr>
<tr>
<td>Analysis Topic</td>
<td>Best Practice</td>
<td>Evaluation</td>
<td>Recommendation</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Control and Authorization Security Testing</td>
<td>Access Control and Authorization Control should be configured to consistently apply the Principle of Least Privilege and minimize the attack surface of the systems.</td>
<td>All access points into the OS 2200 operating system were designed to require authentication, greatly limiting the potential attack surface for unauthenticated attackers. During testing the attack surface was analyzed in detail across the OS 2200 instances and a number of plaintext management protocols were identified. In one example test configuration of both plaintext and encrypted access to the SILAS Administration console was allowed. This was determined to be a deviation from the recommended configuration within the test bed environment and Unisys subsequently remediated the configuration.</td>
<td>Clients should follow the Unisys implementation guides and ensure settings are consistently applied, verified and tested prior to release into a client's production environment.</td>
</tr>
<tr>
<td>Logging and Auditing Assessment</td>
<td>The operating system should be capable of presenting administrators with a log of system activities.</td>
<td>OS 2200 provides an auditing and logging component as an integral part of the operating system. Log analyzer software and Apex log-based reports give system security administrators the ability to view and filter the system log to</td>
<td>No recommendations are necessary for this topic. The systems reviewed either meet or exceed industry best practice, in relation to their ability to effectively record, manage and maintain system event logs.</td>
</tr>
<tr>
<td>Analysis Topic</td>
<td>Best Practice</td>
<td>Evaluation</td>
<td>Recommendation</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Format Fuzzing</td>
<td>Malformed files should be effectively handled by the target program and error gracefully in the event of a program exception.</td>
<td>File format fuzzing is a testing strategy designed to find bugs in native OS 2200 software installed on the systems under test conditions.</td>
<td>Foundstone Consultants were unable to trigger any ineffectively handled behaviors from the target ZIPUT program, during file based fuzzing.</td>
</tr>
<tr>
<td>Apex Management Application Assessment</td>
<td>The Apex management interface, Apex Agent and supporting infrastructure should protect the confidentiality, integrity and availability of the systems and data resources at all times.</td>
<td>A comprehensive web application assessment was undertaken of the elements detailed in Figure 1 (above). These included assessment of the ASP.NET Apex web application and an assessment of the communications between the ASP.NET application and the Apex Agent resident on the OS 2200 servers.</td>
<td>A number of flaws were identified in the ASP.NET Apex web application and remediated. Some of them relate to improper handling of user supplied data within the application. Others were IIS configuration issues and server settings, which are outside the specific scope of this OS 2200 penetration test. Configuration security recommendations are covered by Unisys in the</td>
</tr>
<tr>
<td>Analysis Topic</td>
<td>Best Practice</td>
<td>Evaluation</td>
<td>Recommendation</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Fuzz Testing</td>
<td>The attack surface of the operating system should be minimized. Where services are exposed these should effectively respond and error appropriately when malformed traffic is received, at any stage of the communications.</td>
<td>Two phases of fuzzing were conducted against the elements of the OS 2200 test bed's attack surface. In the first phase a variety of scripts were developed to duplicate the range of client-server conversation and replicate the protocols under test. The second phase of fuzz testing was performed to mimic more comprehensively the potential range of client-server interaction. This was performed using a TCP and UDP redirector to allow the Foundstone testers to manipulate the traffic streams intelligently with fuzz parameters between the legitimate client and the OS 2200 target.</td>
<td>Testing was able to cause some Denial of Service conditions. In collaboration with the Unisys development teams, patches were quickly developed, tested and applied to the test bed for further testing. In all cases the remediation efforts addressed the Denial of Service conditions.</td>
</tr>
</tbody>
</table>
Conclusions

Unisys ClearPath Forward OS 2200 provides Enterprise clients with a robust set of security configuration templates and options from which a customer can select the level of security and the detailed security controls to be applied to the OS 2200 operating system. Throughout testing, architecture and design discussion with Unisys it is evident that the OS 2200 operating system has had security design principles such as “deny by default” and “least privilege” as a foundation throughout its evolution. Administrators can leverage the extensive OS 2200 documentation sets to customize and refine the operating system to meet and exceed a variety of information security objectives. The granularity of management control over system resources within the Security Level 1 systems under review as part of the Foundstone engagement was exceptional.

OS 2200 is also designed to provide a secure environment for program execution which protects against attempts to inject and execute malicious code. OS 2200 access control capabilities allow administrators to employ several means of identifying users and controlling their system access. They also let administrators and resource owners control which users and processes can access data files, execute programs, and manage all of the system’s resources. OS 2200 provides a robust auditing and logging mechanism integrated into the operating system. Extensive logging includes a large number of events that are logged as being either security relevant or security violations, enabling the rapid discovery and forensics of potential attacks. OS 2200 provides an integrated technology stack in which all system components, including resource allocation, system monitoring, and account management have all been designed, implemented, and tested to collaborate and promote system-wide security.

The OS 2200 memory resource management helps mitigate buffer overflow attacks, by preventing user applications from being granted direct memory access. This concept was tested at length across the duration of the Foundstone engagements for Unisys.

In addition to the security controls tested and identified within the OS 2200 operating system, the Foundstone Consultants noted during their review that effective reporting and close collaboration between the ClearPath Forward OS 2200 Operations, Architecture and Development teams within Unisys is in place. During testing it was noted that this culture allows Unisys to respond rapidly and coordinate patches and remediation during the test phases. As with any software platform, administrators and users can greatly affect the overall security.

The OS 2200 environment offers a wide variety of security configuration capabilities and care should be taken to adhere appropriately to the comprehensive, security focused implementation guides provided by Unisys. These documentation sets seek to support clients in their specific OS 2200 configuration scenarios and help clients meet their specific information security objectives.
About McAfee

Technology has the power to enrich the life of everyone. To transform how we live and work. But as technology becomes more deeply integrated into life, security must be more deeply integrated into technology.

By combining the security expertise of McAfee with the innovation, performance, and trust of McAfee, this vision is becoming a reality.

Security that's built-in by design, seamlessly integrated into every device at every layer of the compute stack. Protecting valuable intellectual property, data, devices, and identities. So in everyday and business life, people can feel secure in the digital world.

It's why we're taking a “security connected” approach. Across every architecture of every platform from chip to cloud — smartphones and tablets to PCs, servers, and beyond. We're moving security from discrete solutions to an integrated approach as pervasive as computing itself.

About McAfee Professional Services

Our Worldwide Professional Services organization is ready to respond to the changing needs of global customers and partners seeking security consulting services — from incident response and security risk assessments to comprehensive, customized deployments and training.

Foundstone consultants are seasoned experts skilled at identifying network and application vulnerabilities, providing remediation recommendations, and helping organizations design iron-clad security programs and enforceable policies.

Solution Services consultants are highly skilled at properly planning, designing and implementing security technologies so you can feel confident that you are gaining the most from your investments in McAfee security solutions.

Education Services courseware developers and instructors design and deliver product training and security education to help fortify your security defenses. Customers gain critical skills necessary to deploy and administer their McAfee solutions through formal instructor-led training and self-paced learning opportunities, and then have the opportunity to validate these skills with industry-recognized certifications.