Experience Cyber

Challenge Submission Report

https://range.xpcyber.com/reports/verify/986FD-576D-5EF74/

Submission ID: 134146

Timestamp: 5/1/2025 10:21 PM UTC

Name: Alexander Stewart

Challenge ID: 211

Challenge Title: CISA Threat Sandbox Challenge: ForgeRock OpenAM Backstage Pass (CVE-2021-35464)

This report has not been published by a curator. Experience Cyber cannot vouch for its accuracy.

Scenario

Your mission in this CISA Threat Sandbox Challenge is to learn about CVE-2021-35464, a dangerous remote code execution (RCE) vulnerability, and then exercise that knowledge along with your offensive and defensive cyber skills. You will be provided with real-world, authoritative reference materials that cover details critical to understanding the offensive and defensive angles of this CVE. After learning about the CVE, you will be asked to complete two technical objectives, one red team (offensive) and one blue team (defensive), related to the CVE: Red Team (Offensive) Objective: Utilize CVE-2021-35464 to deploy command and control (C2) enabled malware on a system running a vulnerable ForgeRock OpenAM instance used by an information technology (IT) business (i.e., the red target system). Blue Team (Defensive) Objective: Implement a known mitigation method for CVE-2021-35464 to safeguard a server running a vulnerable OpenAM instance used by an information technology (IT) business (i.e., the blue target system). All exploit code required to complete the Red Team objective will be provided within the workspace.

Duration

0:24

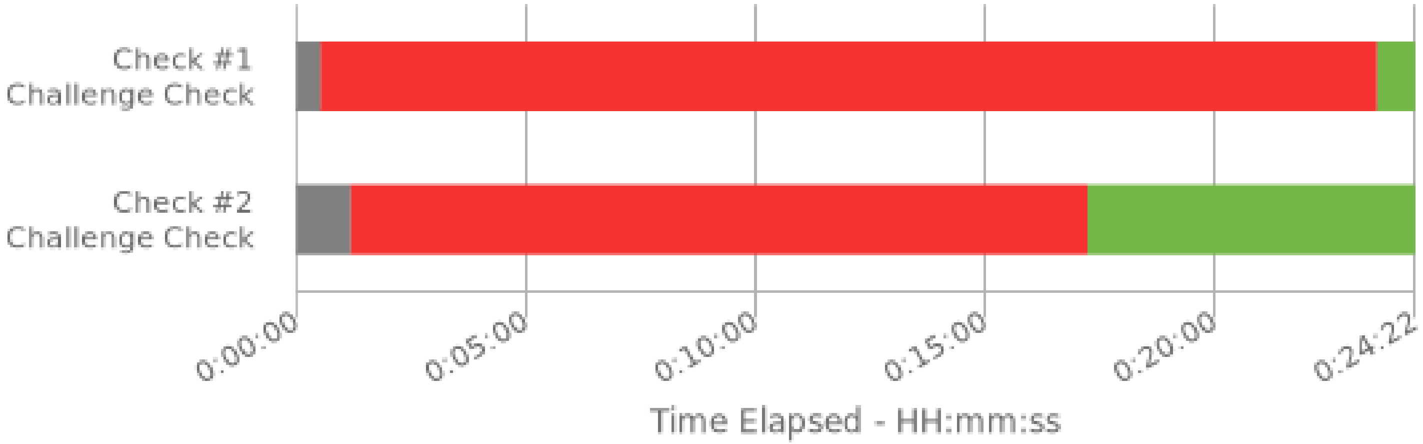
Full Check Pass

Full: 2/2

Final Check Details

✓ Check #1: C2 Listener Deployed on Red Target

✓ Check #2: CVE-2021-35464 Mitigated on Blue Target



Specialty Area

Cyber Operations

Work Role

Cyber Operator

NICE Framework Tasks

- T0696 Exploit network devices, security devices, and/or terminals or environments using various methods or tools.

Knowledge, Skills, and Abilities

- K0005 Knowledge of cyber threats and vulnerabilities.
- K0009 Knowledge of application vulnerabilities.
- K0029 Knowledge of organization's Local and Wide Area Network connections.
- K0034 Knowledge of network services and protocols interactions that provide network communications.
- K0060 Knowledge of operating systems.
- K0070 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- K0088 Knowledge of systems administration concepts.
- K0108 Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
- K0167 Knowledge of system administration, network, and operating system hardening techniques.
- K0373 Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
- K0392 Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
- K0393 Knowledge of common networking devices and their configurations.
- K0395 Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
- K0412 Knowledge of cyber lexicon/terminology
- K0536 Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).
- K0612 Knowledge of what constitutes a “threat” to a network.
- K0625 Knowledge that patching and software updates are impractical for some networked devices.
- S0143 Skill in conducting system/server planning, management, and maintenance.
- S0267 Skill in remote command line and Graphic User Interface (GUI) tool usage.
- S0293 Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.

Centers of Academic Excellence Knowledge Units

- Basic Networking
- Cybersecurity Foundations
- IT Systems Components
- Network Security Administration
- Network Technology and Protocols

- Operating Systems Administration
- Operating Systems Concepts
- Penetration Testing