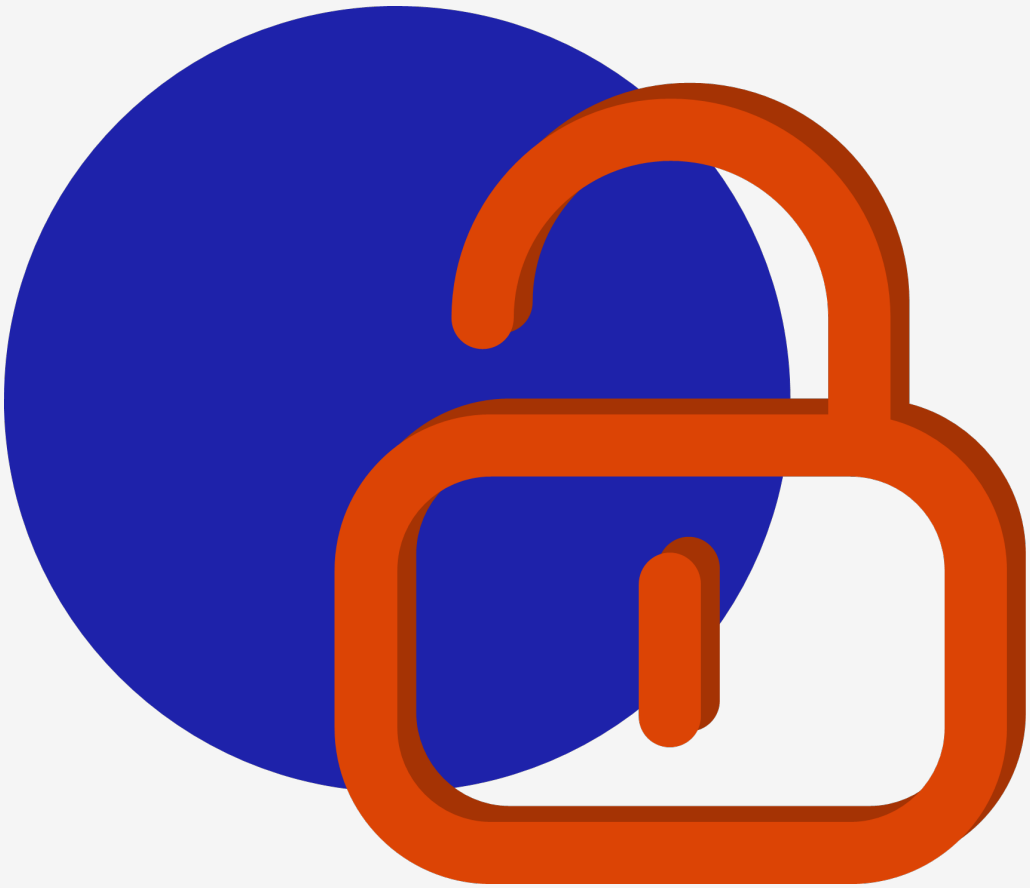
++

Sophos Firewall Security Review: Letter of Attestation

Sophos

28 November 2024



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2024–11–07	Christo Erasmus	Document created	0.1
2024–11–28	Christopher Panayi	Document published	1.0

Document Distribution

Date	Name	Company
2024–11–28	Steven Hedworth	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of the Sophos Firewall Operating System (SFOS), focusing exclusively on the High Availability (HA) and the Up2Date features. This assessment was conducted from the 27th of September to the 6th of November 2024, in conjunction with a security review of the Sophos Connect VPN client. The assessment aimed to identify vulnerabilities in these SFOS components that could be used to compromise or otherwise undermine the security of a firewall device or its users.

2. Approach

The scope of the assessment included the HA and Up2Date features of SFOS, as well as the server component of Up2Date. The assessment followed a white-box approach, with the MWR testing team being given access to source code, documentation and the development team, where relevant.

The assessment approach involved assessing the attack surface of these SFOS features in order to determine the most likely attack vectors, followed by an investigation of their implementation to:

1. understand the architecture and technical implementation of the features,
2. identify the relevant security-related implementation details,
3. establish the presence of vulnerabilities in the features,
4. where present, determine the conditions required for practical exploitation of the vulnerabilities,
5. and to craft Proof of Concept exploits demonstrating the issues to allow for reproduction during remediation efforts.

The in-scope features were assessed from various different perspectives, including:

- Attacks against a firewall device from the networks it is connected to
- Attacks against a firewall device from specific network interfaces that are used by the in-scope features, such as the dedicated link used for HA
- Meddler-in-the-Middle (MitM) attacks between a device and Sophos' servers, or between two devices communicating with each other
- Attacks relying on limited, or temporary, physical access to a device
- Attacks relying on limited, or temporary, access to a device's administration interfaces

3. Results

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
High-Availability Feature Security Review	0	3	4	0
Up2Date Security Review	0	0	4	1
Total	0	3	8	1

A small number of viable attack paths targeting the HA feature were identified during the assessment. Based on MWR's investigations, and discussions with the Sophos development team, effective remediation of these was considered to require a low amount of development work. In general, it was clear that efforts had been made to minimise this feature's attack surface and further architectural considerations in this line were provided to Sophos after the assessment. Throughout the assessment, the SFOS development team was observed to be proactive regarding the security testing conducted and, several times during the engagement, asked for specific test cases to be performed in order to ensure the thoroughness of the review.

The vulnerabilities identified in the Up2Date system were not deemed to pose a significant risk, as they had limited impact and could only be exploited in specific conditions. Most of these vulnerabilities were expected to be relatively simple to resolve. No security vulnerabilities were identified in the most critical components of Up2Date, and based on a review of the source code and documentation it was clear that these components were developed in a way that minimised their attack surface and hardened the firewall's update process against attack.

Risk Rating Scale

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos' electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Project Team

Assessment Team

Lead Consultant	Christopher Panayi
Additional Consultants	Christo Erasmus Connor du Plooy

Quality Assurance

QA Consultants	Momelezi Mchunu Johan van der Merwe Matthew Bouffé Mohammad Pathan Stephen Munro

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC