IOActive Security Advisory

Title	Fortinet FortiGate – Cross-site Scripting in SSL VPN
Severity	High
Discovered by	Jamie Riden
CVE	CVE-2024-26006
Advisory Date	2024-07-25

Affected Products

Version	Affected
FortiOS 7.4	7.4.0 through 7.4.3
FortiOS 7.2	7.2.0 through 7.2.7
FortiOS 7.0	7.0.0 through 7.0.13
FortiOS 6.4	6.4 all versions
FortiProxy 7.4	7.4.0 through 7.4.3
FortiProxy 7.2	7.2.0 through 7.2.9
FortiProxy 7.0	7.0.0 through 7.0.16

Background

Fortinet, Inc. (Fortinet) is a global leader of cybersecurity solutions and services that provides protection against cyber threats. It is a company that develops and sells security products and solutions, such as firewalls, endpoint security, intrusion prevention systems, web filtering, antivirus, sandbox, and VPN.

FortiGate is a network security device that provides protection against cyber threats. The device can perform various functions, such as, firewall, intrusion prevention system, web content filtering, antivirus, sandbox and VPN and is part of the Fortinet Security Fabric, which integrates different security products and services into a unified and automated platform.

Timeline

- 2023-11-16: IOActive discovers the vulnerability
- 2023-11-22: IOActive informs Fortinet about the identified vulnerability
- 2024-01-12: Fortinet acknowledges the issue
- 2024-04-26: CVE ID pre-reserved by Fortinet

- 2024-07-10: Advisory published by Fortinet
- 2024-07-25: IOActive advisory published

Threat and Impact

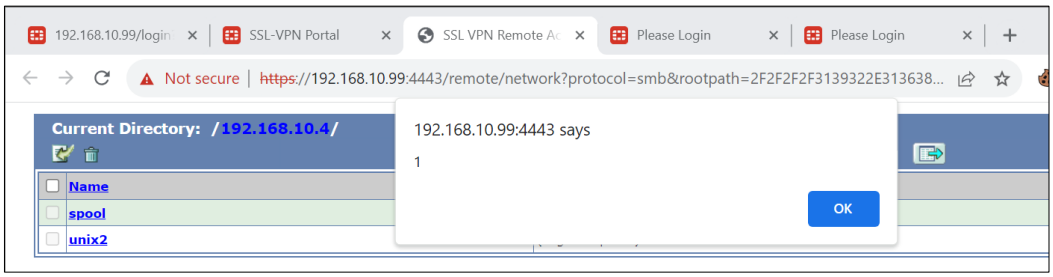
If a user with access to SSL VPN in web mode can be enticed into connecting to a malicious SMB server, the operator of the malicious server can cause JavaScript code execution via cross-site scripting (XSS) from the `Comment` field of the SMB share.

Proof of Concept

The following Samba configuration was implemented on a Linux server, 192.168.10.4, so that the XSS string was in the `Comment` field of the SMB share.

```
[unix2]
  comment = "<img src=i onerror=alert(1)>"
  path = /home/ubuntu
  guest ok = yes
...
```

The SSL VPN was then used to connect to the root of the SMB server, `smb://192.168.10.4/`, which triggered the execution of the JavaScript in the comment field:



By changing the `Comment` field of the SMB share to:

```
comment = "\"]';
window.location.href=String.fromCharCode(0x2f)+String.fromCharCod
e(0x2f)+'bbc.co.uk'; var a='"
```

It was possible to cause a redirect to `https://bbc.co.uk`, which could in practice be used to redirect users to a phishing website.

Recommendation

The `Comment` field of an SMB share needs to have the same output encoding that is applied to pathnames, etc.

