

Content Type	Description
Title	<i>Critical Vulnerability in Fortinet Firewalls and Proxies</i>
Id	202210/Alert/06
Code LTP	White
Risk Level	<b>Critical</b>
Application and service has been designed	<b>FortiOS, FortiProxy and FortiSwitchEach</b>
Version	<ul style="list-style-type: none"> <li>- FortiOS version 7.2.0 to 7.2.1 and version 7.0.0 to 7.0. 7</li> <li>- FortiProxy version 7.2.0 and version 7.0.0 to 7.0.6</li> <li>- FortiSwitchManager version 7.2.0 and 7.0.0</li> </ul>
Platform	<b>Fortinet</b>
Update	<ul style="list-style-type: none"> <li>- FortiOS versions 7.0.7 and 7.2.2</li> <li>- FortiProxy version 7.0.7 et 7.2.1</li> <li>- FortiSwitchManager version 7.2.1</li> </ul>
Summary	<i>A security vulnerability affecting FortiGate x firewalls and FortiProxy web proxies that could potentially allow attackers to perform unauthorized actions on sensitive devices.</i>
Impacts	<ul style="list-style-type: none"> <li>- Access to sensitive equipment</li> </ul>
Detailed Description	<p><i>On Monday, October 10, 2022, Fortinet revealed a critical security vulnerability affecting its firewall and proxy products.</i></p> <p><i>The vulnerability referred to as CVE-2022-40684 (CVSS score: 9.6) concerns <b>an authentication bypass</b> in FortiOS, FortiProxy, and FortiSwitchManager that could allow a remote attacker to perform unauthorized operations on the administration interface via specially crafted HTTP or HTTPS requests.</i></p>
Solutions	<p><i>Fortinet has released security updates in FortiOS versions 7.0.7 and 7.2.2, FortiProxy versions 7.0.7 and 7.2.1, and FortiSwitchManager version 7.2.1.</i></p> <p><i>If updating to the latest version is not possible, it is recommended that users disable the HTTP/HTTPS administration interface, or limit the IP addresses that can access the administration interface.</i></p>
Links for more details	<p><i><a href="https://www.fortiguard.com/psirt">https://www.fortiguard.com/psirt</a></i></p> <p><i><a href="https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy">https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy</a></i></p>