CVE-2022-22954 PoC - VMware Workspace ONE Access Freemarker Server-Side Template Injection

Executive Summary	
VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. A malicious actor with network access could trigger a server-side template injection that could result in remote code execution. The PoC has been published and should be used with great care. In addition, VMware has confirmed that it is Exploited in the Wild.	
Introduction	
Vulnerability Details: This vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware Workspace ONE Access. Authentication is not required to exploit this vulnerability. A particular flaw is found in the customError.ftl template. A vulnerability classified as very critical was found in Vmware Workspace ONE Access and Identity Manager. The affected component is the Template Handler. A Remote Code Execution Vulnerability has been found in VMware Workspace ONE Access customError.ftl Server Side Template Insertion.	
Impact of Vulnerability	
System Compromise: Remote attackers can take control of vulnerable systems. Affected Products: VMware Workspace ONE Access 20.10.0.1, 20.10.0.0, 21.08.0.1, 21.08.0.0 VMware Identity Manager 3.3.6, 3.3.5, 3.3.4, 3.3.3 VMware Cloud Foundation (vIDM) 4.x vRealize Suite Lifecycle Manager (vIDM) 8.x VMware Realize Automation 7.6	
Description of Abuse	
Indicates an attempt to attack the Server-Side Template Injection vulnerability in VMware Workspace ONE Access and Identity Manager. **Details are below:** CVSS key metrics Critical 9.8 Attack vector Network Attack complexity Low No required privileges No user interaction Without Changing Scope Privacy High Integrity High Availability High	
Current Status of Abuse	
The first PoC was also published on GitHub the same day by sherlocksecurity. The public proof-of-concept exploit code is available and would even fit in a tweet. https://github.com/sherlocksecurity/VMware-CVE-2022-22954 https://github.com/DrorDvash/CVE-2022-22954_VMware_PoC https://twitter.com/wvuuuuuuuuuuuuu/status/1519476924757778433 https://twitter.com/bad_packets/status/1514293472697585669	

Mitigation Suggestions	
Apply the latest upgrade or patch from the vendor. https://www.vmware.com/security/advisories/VMSA-2022-0011.html CVE-ID CVE-2022-22954, GHSA-ID GHSA-q7xc-35g4-g566	
Decision	
VMware customers should immediately patch their installations of Workspace ONE Access and Identity Manager without waiting for a regular patch cycle to occur. The vulnerability is caused by insufficient protection of custom templates provided by the user. A remote attacker could exploit this to execute arbitrary code in the context of the target system.	
References:	
https://nvd.nist.gov/vuln/detail/CVE-2022-22954 https://nvd.nist.gov/vuln/detail/CVE-2022-22954 https://core.vmware.com/vmsa-2022-0011-questions-answers-faq # https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21954 https://github.com/advisories/GHSA-q7xc-35g4-g566	