AD Privilege Escalation

2 vulnerabilities that can lead to easy Windows domain takeover

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699
CVEs: CVE-2021-42287 CVE-2021-42278

On November 9, Microsoft released a patch for several zero-day vulnerabilities related to Active Directory privilege escalation, 2 of which are of particular interest as they can lead to Windows Domain takeover when chained together.

Background

As reported by Microsoft - during the November security update cycle, a patch was released for vulnerabilities CVE-2021-42287 and CVE-2021-42278. Both vulnerabilities are described as a 'Windows Active Directory domain service privilege escalation vulnerability'. When combining 42287 and 42278, an attacker can create a straightforward path to a Domain Admin user in an Active Directory environment that hasn't applied these new updates. This escalation attack allows attackers to easily elevate their privilege to that of a Domain Admin once they compromise a regular user in the domain. On December 12, 2021, a proof-of-concept tool leveraging these vulnerabilities was publicly disclosed.

Announced

The initial patch and vulnerability disclosure was published at:

https://thehackernews.com/2021/11/microsoft-issues-patches-for-actively.html

Follow-up guide from Microsoft following the proof-of-concept disclosure is available at:

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699

Latest Developments

Active POC code is circulating in the wild, and Active Directory administrators are strongly encouraged to upgrade immediately. The Fortinet Security Fabric protections below can help detect the vulnerability, prevent exploit, or hunt for indicators related to these vulnerabilities across the attack surface.

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*19.234*	Blocks attempts to exploit the Active Director Privilege Escalation.
FortiClient	**Vulnerability**	*1.276*	Detects the presence of the Active Directory Privilege Escalation vulnerabilities, and applies auto-patching if enabled.
	Application Firewall	*19.234*	Blocks attempts to exploit the Active Director Privilege Escalation.
FortiEDR	**Pre-Execution**	*5.0.2.335+*	Blocks attempts to exploit the Active Director Privilege Escalation.
	Post-Execution	*5.0+*	Out-of-the-box, EDR blocked the proof-of-concept weaponization-prior to its public disclosure on Dec 12.
FortiDeceptor	**Decoy**	*3.3+*	Detects activities related to the Active Directory Privilege Escalation attack
FortiADC	**IPS**	*19.234*	Blocks attempts to exploit the Active Director Privilege Escalation.
FortiProxy	**IPS**	*19.234*	Blocks attempts to exploit the Active Director Privilege Escalation.
FortiAnalyzer	**Outbreak Detection**	*1.00045*	Detects indicators of the AD Privilege Escalation vulnerability from across the Security Fabric
	Threat Hunting	*6.4+*	Detects indicators of the AD Privilege Escalation vulnerability from across the Security Fabric

Cyber Kill Chain

Reconnaissance

FortiDeceptor
Decoy
Version Info: 3.3+
Link: https://community.fortinet.com/t5/FortiDeceptor/Technical-Tip-How-to-use-FortiDeceptor-to-detect-Active/ta-p/201949

Weaponization

Delivery

FortiClient
Vulnerability
Version Info: 1.276
Link: https://www.fortiguard.com/updates/epvuln?version=1.276

Exploitation

FortiGate
IPS
Version Info: 19.234
Link: https://www.fortiguard.com/updates/ips?version=19.234

FortiClient
Application Firewall
Version Info: 19.234
Link: https://www.fortiguard.com/updates/ips?version=19.234

FortiEDR
Pre-Execution
Version Info: 5.0.2.335+
Link: https://www.fortinet.com/blog/threat-research/cve-2021-42278-cve-2021-42287-from-user-to-domain-admin-60-seconds

FortiADC
IPS
Version Info: 19.234
Link: https://www.fortiguard.com/updates/ips?version=19.234

FortiProxy
IPS
Version Info: 19.234
Link: https://www.fortiguard.com/updates/ips?version=19.234

Installation

FortiEDR
Post-Execution
Version Info: 5.0+
Link: https://www.fortinet.com/blog/threat-research/cve-2021-42278-cve-2021-42287-from-user-to-domain-admin-60-seconds

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
Outbreak Detection
Version Info: 1.00045
Link: https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00045

Threat Hunting
Version Info: 6.4+
Link: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-activities-related/ta-p/201964