Security Advisory GOVSA.2022.0506.1 – Temporary disabling and enabling of the Windows Firewall during a remote Goverlan Agent update

Advisory ID	GOVSA.2022.0506.1
Vulnerability Type	CWE-1038 Insecure Automated Optimizations
Issue Date	2022-05-16
Updated On	2022-05-06 (Initial Advisory)
Application	Goverlan Reach (Agent)
Affected Versions	Goverlan Reach Console v10.5.0 and earlier Goverlan Client Agent v10.1.10 and earlier
Severity	Medium
Vulnerability Status	Update Released
CVE Status	Submitted – CVE Record | CVE

Summary

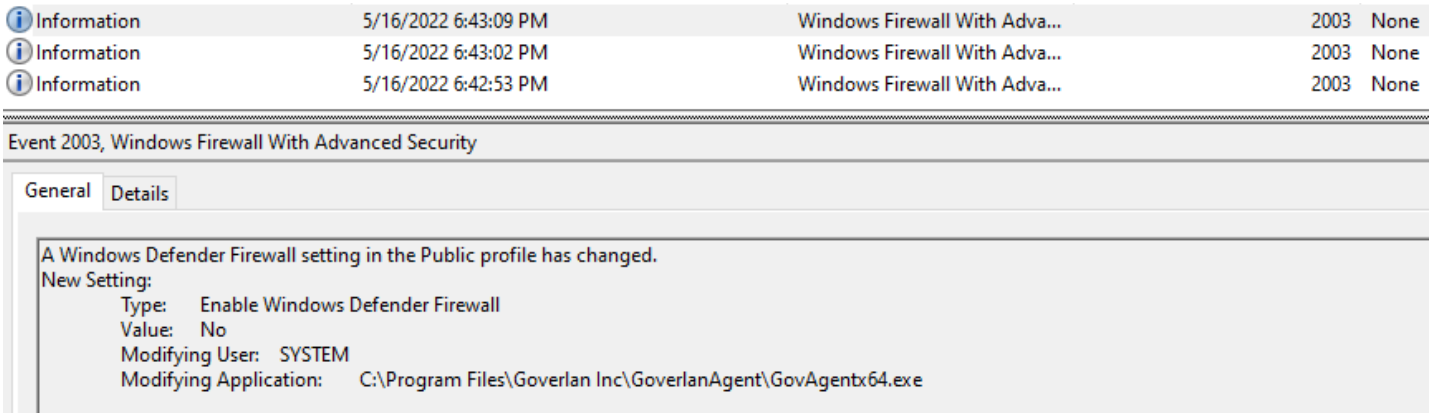
The Windows Firewall is temporarily turned off upon a Goverlan agent update operation in Goverlan Management Console v10.5.0, Goverlan Reach Server v3.70.0 and earlier versions, which allows remote attackers to bypass firewall blocking rules for a time period up to 30 seconds.

Vulnerability Type	Remotely exploitable	Impact
Insecure Automated Optimizations	No	A remote system loses Windows Firewall protection for up to 30 seconds.

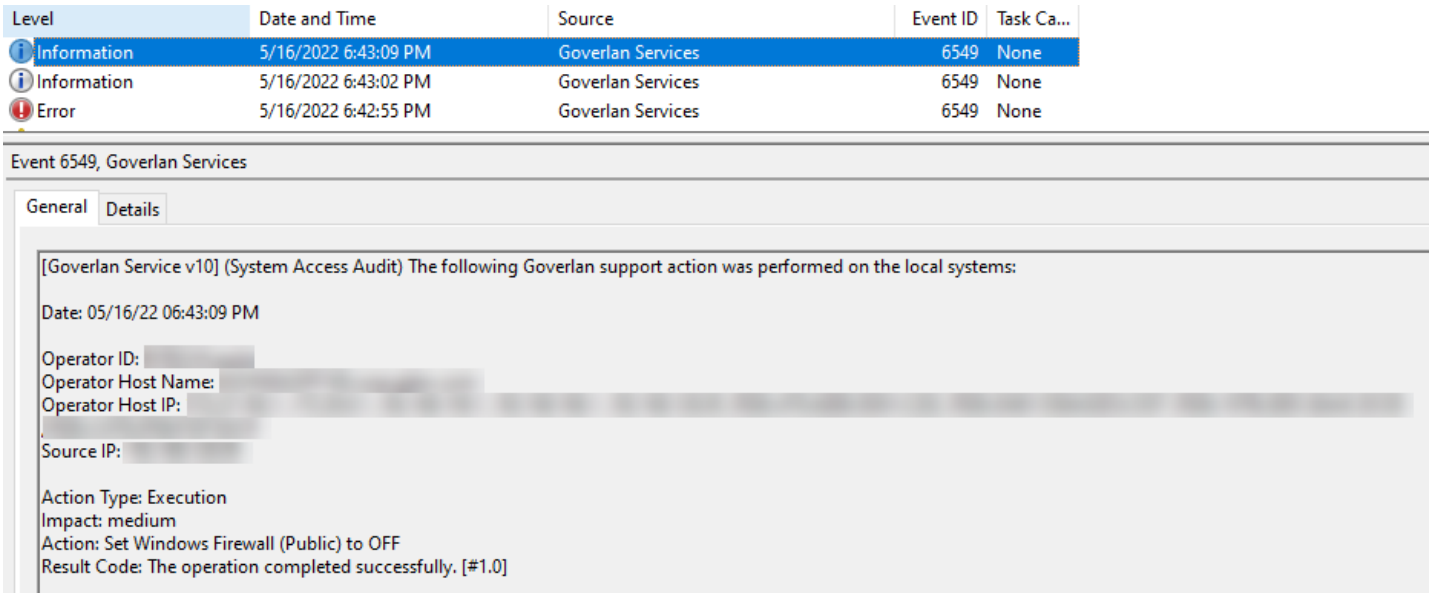
Detection

This behavior can be detected by the presence of one Windows Event that is not accompanied by a Goverlan Reach Audit Event. If both events are present, the action was performed using the Goverlan Reach consoles feature. If the Firewall Event ID 2003 is the only event present and the Modifying Application is GovAgent64.exe then this vulnerability is present.

The Windows Event viewer records **Event ID 2003** when the Windows Firewall has been enabled or disabled.



the action listed in the Event.



Goverlan Auditing

The Goverlan Reach Agents are designed to monitor all configuration changes that are performed on a system by Goverlan Operators. All audits are contained in the Windows Event Viewer of the endpoint system. We recommended using a SEIM product at the endpoint to detect Goverlan Reach related events. See Goverlan Reach Auditing for more information.

Relevant Products

This vulnerability is exposed by the Goverlan Agent process: GovAgentx64.exe and GovAgent.exe versions **10.1.10** and earlier.

These Goverlan Client Agent are distributed on remote machine via the Goverlan Reach Console and Goverlan Reach Server versions **10.5.0** and **3.70.0** and earlier respectively.

Remediation

Goverlan Client Agent v10.1.10 and earlier	Update to v10.1.11 or later

Contacts

For further information about this security advisory, or to send us a security alert, please contact security(@)goverlan.com.

Updated on May 23, 2022

Tagged: Security Advisory