Improved Server Security with iDRAC9 and SELinux

Abstract

Dell EMC 14th generation PowerEdge servers offer greater risk mitigation in iDRAC9 using SELinux. This document introduces the new security features in iDRAC9.

September 2018

Revisions

Date	Description
September 2018	Initial release

Acknowledgements

This paper was produced by the following members of Dell EMC:

Author: Florin Dragan, Michael E Brown

Support: Kang Quan, Neel Parikh

Other: Doug Iler, Nazira Carlage

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of contents

Executive summary

This whitepaper introduces two new security initiatives that Dell EMC is providing in iDRAC9; SELinux and ‘non-root least privileges’. This whitepaper explains what these initiatives are, what Dell EMC did to implement them, and how they enhance customer experience by increasing the security of the embedded controllers. Finally, some examples of historical vulnerabilities in iDRAC8 are provided and followed by how the new initiatives protect the customers if similar vulnerabilities are found in iDRAC9.

1 Overview

All Dell EMC PowerEdge servers contain an Integrated Dell Remote Access Controller (iDRAC). iDRAC enables seamless remote management of the server. 14th generation PowerEdge servers are shipped with the iDRAC9. iDRAC is essentially a computer subsystem that runs inside the server and can remotely control the server and re-install the operating system, among other features. Because of its extensive capabilities, hackers are incentivized to hack iDRAC to gain control over the system. With iDRAC9, we have been adding new security enhancements. The recent release of iDRAC 3.21.21.21 was a culmination of several key security initiatives that Dell EMC has been working on for several years. These enhancements are designed to protect users from attackers who try to gain access to their servers using iDRAC. We believe that these are industry-leading technologies in security for embedded management.

2 Security initiatives

2.1 SELinux framework

The first initiative is the adoption of the SELinux security framework. Dell EMC wrote comprehensive security policies for every task that runs on the iDRAC and then ran comprehensive tests to ensure that no features were broken in the process. SELinux operates at the core kernel level on the iDRAC and does not need any input or configuration from the users. SELinux adds a mitigation factor that prevents many programming flaws from being further exploited to gain elevated access to the system. Moreover, SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. Currently, these logs are available through SupportAssist to customers enrolled in this new feature. In future release of iDRAC, these logs will be available in the Lifecycle Controller Logs.

SELinux is a core Linux security technology that is merged in the standard Linux kernel. SELinux has been gaining adoption within many Linux distributions. Red Hat Enterprise Linux (RHEL) was one of the first adopters other Linux users followed. SELinux is now maintained in the core Linux kernel by a dedicated group including Red Hat, Network Associates, Secure Computing Corporation, Tresys Technology, among others. This security technology uses a method referred to as *Mandatory Access Control*. This method enables you to specify all the privileges that internal processes need to complete their tasks and also limits the access to only those tasks. This is important because most attempts to hack a system involve trying to make processes do things that are outside of the original design.

2.2 Processes with Unix root privilege

The other major initiative is to eliminate processes that run with Unix *root* privileges. IDRAC was originally ported from an OS that did not have the concept of user privilege separation and that remnant lasted for several generations. Dell EMC has undertaken a major initiative to ensure that all internal processes running inside iDRAC run with the least-required privileges; a core Unix security concept. This approach provides protection against programming flaws. This protection ensures that the process of a system that might get attacked cannot access files or hardware that are outside the scope of that process. For example, the process that provides Virtual KVM support should not be able to change fan speeds. Running these two processes as different users helps protect the system by preventing attacks from propagating from one process to another.

3 Customer impact

Together, these two initiatives offer defense against security threats and malicious attacks against iDRAC9. These security measures result in better protection of customer's assets. Adding SELinux is a proactive measure to increase security of Dell EMC embedded systems management tools.

However, it should be noted that SELinux constrains and mitigates certain classes of exploits but does not prevent them. An analogy would be that if a vulnerability is exploited, SELinux confines the attacker to a very limited safe room and makes it more difficult for an attacker to fully compromise the system. A system with SELinux is much harder to break into when compared to a system without SELinux. Some of the vulnerabilities can be mitigated effectively by SELinux, including the following:

- Shellshock
- A few recent Samba privilege escalation and remote code execution attacks
- A few Apache privilege escalation and path traversal

Dell EMC is proactive in implementing security measures. Instead of waiting for vulnerabilities to be discovered and then patching them, Dell EMC now implements SELinux and 'non-root least privileges' to provide restricted and authorized access, thereby limiting what attackers can do. SELinux is best-of-breed security to protect the system in the event of an attack. It can confine behavior of attackers, mitigate the consequences of a security breach, and potentially turn what could be a catastrophic breach into a minor one.

3.1 Security considerations

If we test historical security vulnerabilities in a system with non-root access and SELinux enabled, we see the types of attacks or security issues that these initiatives can be expected to prevent. These tests also help in identifying the types of security issues that are not addressed.

In the following sections, a few examples of security issue found in previous versions of iDRAC are listed. The list also provides details on how these security initiatives helped in mitigating those issues. As with any security technology, SELinux and non-root are not panaceas, and cannot protect against every conceivable flaw. Therefore, we also give examples of some historical vulnerabilities that cannot be mitigated with SELinux and non-root access.

3.2 Security issues mitigated by SELinux and non-root privilege

Following is a list of some of the vulnerabilities found in previous generation of iDRAC. SELinux can either partially or fully mitigate these issues. Details are also provided about impact if the same vulnerabilities are encountered in iDRAC9. The intent is to show examples of vulnerabilities that SELinux mitigates fully or partially, and the ones that it cannot mitigate. These issues have been addressed in the latest releases of iDRAC.

- CVE-2018-1207: Dell EMC iDRAC7/8
  Versions earlier than iDRAC 2.52.52.52 contain CGI injection vulnerability that could be used to execute remote code. A remote unauthenticated attacker may potentially be able to use CGI variables to execute remote code.
- CVE-2018-1207: Dell EMC iDRAC9
  CGI injection vulnerability in iDRAC7/8 could allow an attacker to execute arbitrary OS commands on iDRAC because the CGI scripts used to run with root privileges. If a similar injection vulnerability is found in iDRAC9, the impact would be greatly reduced. With SELinux

enabled, the web server processes in iDRAC9 do not run under root user and are configured to have limited access to system files.

- CVE-2018-1211: Dell EMC iDRAC7/8
  Versions earlier than iDRAC 2.52.52.52 contain a path traversal vulnerability in the web server's URI parser that could be used to obtain specific sensitive data without authentication. A unauthenticated remote attacker might have been able to read configurations settings from the iDRAC by querying specific URI strings.
- CVE-2018-1211
  Due to a programming error in the code, this path traversal vulnerability in IDRAC7/8 could allow an attacker to remotely access arbitrary files in the IDRAC OS. If a similar vulnerability is found in iDRAC9, the impact would be greatly reduced because SELinux is configured to significantly limit the number of files that web server can access. The web server process no longer runs as root. Both SELinux and UNIX permissions restrict access to many files. Sensitive files, such as passwords and config database files, cannot be accessed using this vulnerability.
- CVE-2018-1000116: Dell EMC iDRAC7/8
  iDRAC 7/8 versions earlier than 2.52.52.52 and iDRAC9 versions earlier than 3.20.20.20 contain a heap corruption vulnerability in the NET-SNMP service (an open source component) which could be used to corrupt the heap memory. A remote unauthenticated attacker may be able to send malformed PDUs to the NET-SNMP service and trigger a heap corruption.
- iDRAC9: This is partially mitigated as SNMP process is one of the few processes still running as root. However, the SELinux security policy for SNMP restricts access to many important system files. Dell EMC has released an updated iDRAC version that mitigates this vulnerability by updating SNMP code. If a similar vulnerability is found in future iDRAC releases, this vulnerability would be mitigated using a combination of SELinux policy and 'non-root least privilege'.

3.3 Security issues not mitigated by SELinux and non-root privilege

There are issues that SELinux and 'non-root least privilege' cannot mitigate, and it is important that users understand these limitations.

The issues below are examples of past vulnerabilities discovered in IDRAC that SELinux and 'non-root least privileges' do not mitigate effectively. These examples are provided for illustrative purposes only so that users can see the limitations of SELinux protection.

- CVE-2018-1249
  iDRAC9 versions earlier than 3.21.21.21 did not enforce the use of TLS/SSL for a connection to iDRAC web server for certain URLs. An attacker could use this vulnerability to strip the SSL/TLS protection from a connection between a client and a server. SELinux cannot mitigate this vulnerability because it does not involve access to system files.
- CVE-2018-1243
  iDRAC6 versions earlier than 2.91, iDRAC7/8 versions earlier than 2.60.60.60, and iDRAC9 versions earlier than 3.21.21.21 contain a weak CGI session ID vulnerability. The sessions invoked through CGI binaries use 96-bit numeric-only session ID values, which makes it easier for remote attackers to perform brute-force session guessing attacks. SELinux cannot mitigate this vulnerability issue because it does not involve access to system files.

In closing, this whitepaper has informed users on the new security enhancements that Dell EMC added to iDRAC9. We have outlined SELinux and 'non-root least privilege' initiative and have shown how these technologies can help protect customers' systems from attacks. We have also given examples of historical security vulnerabilities in earlier version of iDRAC that would be mitigated if they were to occur in iDRAC9. And finally, we have shown some examples of limitations of these technologies.