Security Alert 59336: Users with shell access can modify the script file

Summary

The AppDynamics Standalone Machine agent sets file permissions for the script file “extend-os-version.sh” to 777.

This allows any user with shell access to the server to change the script file, which will be executed by the Machine Agent with the level of permissions assigned to the Machine Agent at startup. As a result, any user can obtain elevated admin privileges on a server running the standalone machine agent.

Affected Software

Product	Component	Version	Exploitability	Severity
Machine Agent	AppDynamics Standalone Machine Agent	• 3.5, 3.6, 3.7, 3.8, 3.9 versions • 4.0 versions below 4.0.8.4 • 4.1 versions below 4.1.8.2	Medium	High

Key/Legend for Ratings and Vulnerabilities

Exploitability Rating	Description
Known	AppDynamics is aware of a known exploit. Customers should treat known exploits with the highest priority.
High	AppDynamics believes there is a high probability that a vulnerability is exploitable by an attacker.
Medium	AppDynamics believes there is a moderate probability that a vulnerability is exploitable by an attacker.
Low	AppDynamics believes there is a low probability that a vulnerability is exploitable by an attacker.

Severity Rating	Description
High	Exploit allows an attacker to compromise confidentiality, integrity, accountability, or availability of user data, or of the integrity or availability of processing resources without any mitigations like notifications, audits, and/or authentication.
Medium	Exploit allows an attacker to compromise confidentiality, integrity, accountability, or availability of user data, or of the integrity or availability of processing resources with reasonable mitigations like notifications, and/or authentication mechanisms.
Low	Exploit allows an attacker to compromise confidentiality, integrity, accountability, or availability of user data, or of the integrity or availability of processing resources, however, significant mitigations like notifications, and/or authentication mechanisms are in place to reduce severity of the impact.

FAQ

Q: What do I need to do to protect against this vulnerability?

A: Upgrade the Standalone Machine Agent (Java)

Q: Do I need to upgrade my agents?

A: Yes, the Standalone Machine Agent

Vulnerability Information

The defect allows any user with shell access to modify the script file and therefore execute the changed content with root privileges.

Mitigating Factors and Workarounds

Upgrade to a patched version.

Patched Versions

- https://download.appdynamics.com/browse/zone/3/?version=4.0.8.4
- https://download.appdynamics.com/browse/zone/3/?version=4.1.8.2

Disclaimer

The information provided in this security advisory is provided “as is” without warranty of any kind. AppDynamics disclaims all representations or warranties, either express, implied, statutory, or otherwise with respect thereto, including the warranties of merchantability and fitness for a particular purpose. In no event shall AppDynamics, its affiliates, or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits, or special damages, even if the other party has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply to you.

Revision History

1.0 - 1/26/2016 Initial Revision