IOActive

IOActive Security Advisory

Title	Lenovo's System Update Uses a Predictable Security Token
Severity	High
Discovered by	Michael Milvich michael.milvich@ioactive.com Sofiane Talmat sofiane.talmat@ioactive.com
CVE	CVE-2015-2219
Advisory Date	April 14, 2015

Affected Product

Lenovo System Update (5.6.0.27 and earlier versions)

Impact

This vulnerability allows local least-privileged users to run commands as the SYSTEM user.

Background

The Lenovo System Update allows least privileged users to perform system updates. To do this, the System Update includes the System Update service (SUService.exe). This service runs privileged as the SYSTEM user and communicates with the System Update which is running as the unprivileged user. The service creates a named pipe through which the unprivileged user can send commands to the service. When the unprivileged System Update needs to execute a program with higher privileges, it writes the command to the named pipe, and the SUService.exe reads the command and executes it.

Technical Details

Arbitrarily executing commands sent by a malicious unprivileged user represents a massive security risk. Lenovo does attempt to restrict access to the System Update Service by requiring clients of the named pipe to authenticate by including a security token with the command the unprivileged user wishes to execute. Unfortunately this token is a predictable token and can be generated by any user without requiring any elevated permissions.

As a result, an attacker who is unprivileged can perform the same operations as the System Update. The attacker can create a valid token and include it with a command to be executed. The SUService.exe will then execute the command as the SYSTEM user.

Fixes

Lenovo has released an updated version, which replaces the token authentication method, and is available through the System Update.

Timeline

- February 2015: IOActive discovers vulnerability
- February 19, 2015: IOActive notifies vendor
- April 3, 2015: Vendor releases patch
- April 14, 2015: IOActive and vendor release advisory

IOActive Security Advisory

Title	Lenovo’s System Update Signature Validation Errors
Severity	High
Discovered by	Michael Milvich michael.milvich@ioactive.com Sofiane Talmat sofiane.talmat@ioactive.com
CVE	CVE-2015-2233
Advisory Date	April 14, 2015

Affected Products

Lenovo System Update (5.6.0.27 and earlier versions)

Impact

Local and potentially remote attackers can bypass signature validation checks and replace trusted Lenovo applications with malicious applications. These applications will then be run as a privileged user.

The System Update downloads executables from the Internet and runs them. Remote attackers who can perform a man in the middle attack (the classic coffee shop attack) can exploit this to swap Lenovo’s executables with a malicious executable. The System Update uses TLS/SSL to secure its communications with the update server, which should protect against “coffee shop” style attacks.

Background

The System Update downloads executables from the Internet and runs them. As a security measure Lenovo signs its executables and checks the signature before running them, but unfortunately does not completely verify them.

Technical Details

When performing the signature validation, Lenovo failed to properly validate the CA (certificate authority) chain. As a result, an attacker can create a fake CA and use it to create a code-signing certificate, which can then be used to sign executables. Since the System Update failed to properly validate the CA, the System Update will accept the executables signed by the fake certificate and execute them as a privileged user.

Fixes

Lenovo has released an updated version, which validates the CA chain, and is available through the System Update.

Timeline

- February 2015: IOActive discovers vulnerability
- February 19, 2015: IOActive notifies vendor
- April 3, 2015: Vendor releases patch
- April 14, 2015: IOActive and vendor publish advisory

IOActive Security Advisory

Title	Lenovo's System Update Race Condition
Severity	High
Discovered by	Michael Milvich michael.milvich@ioactive.com Sofiane Talmat sofiane.talmat@ioactive.com
CVE	CVE-2015-2234
Advisory Date	April 14, 2015

Affected Products

Lenovo System Update (5.6.0.27 and earlier versions)

Impact

This vulnerability allows local unprivileged users to run commands as an administrative user.

Background

The System Update downloads executables from the Internet runs them. The System Update does check for a signature before running them, but does so in a directory writable by any user.

Technical Details

As a result of saving the executables in a writable directory, Lenovo created a race condition between verifying the signature and executing the saved executable. A local attacker could exploit this to perform a local privilege escalation by waiting for the System Update to verify the signature of the executable, and then swapping out the executable with a malicious version before the System Update is able to run the executable. When the System Update gets around to running the executable, it will run the malicious version, thinking it was the executable that it had already verified. An attacker can use this to gain elevated permissions.

Fixes

Lenovo has released an updated version, which changes how downloaded files are stored. It is available through the System Update.

Timeline

- February 2015: IOActive discovers vulnerability
- February 19, 2015: IOActive notifies vendor

- April 3, 2015: Vendor releases patch
- April 14, 2015: IOActive and vendor publish advisory