Keysight Technologies Sensor Management Server Multiple RCE Vulnerabilities

Critical

← View More Research Advisories

Synopsis

CVE-2022-38129 - addLicenseFile Path Traversal RCE (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

A path traversal vulnerability exists in the com.keysight.tentacle.licensing.LicenseManager.addLicenseFile() method in the Keysight Sensor Management Server (SMS). This allows an unauthenticated remote attacker to upload arbitrary files to the SMS host.

The attacker can remotely invoke the addLicenseFile() method via URL endpoint /server/service/licensingServiceHttpInvoker. The method takes in the license file name as input data and the file is supposed to be saved in <SMS_DIR>\licenses\, where <SMS_DIR> is the SMS installation directory.

The method checks if the license file name contains a Windows file separator to ensure the file is saved in <SMS_DIR>\licenses\:

```
// com.keysight.tentacle.licensing.LicenseManager.addLicenseFile()
 public LicenseError addLicenseFile(LicenseDescription paramLicenseDescription) {
  if (paramLicenseDescription == null)
   return LicenseError.INVALID_FILENAME;
  String str = paramLicenseDescription.getFilename();
  if (str == null || str.length() == 0)
   return LicenseError.INVALID_FILENAME;
  if (str.contains(File.separator))
   return LicenseError.PATHNAME_NOT_ALLOWED;
  File file = new File("licenses/" + str);
  FileOutputStream fileOutputStream = null;
  LicenseError licenseError = LicenseError.UNKNOWN;
  BufferedOutputStream bufferedOutputStream = null;
  try {
    fileOutputStream = new FileOutputStream(file);
    bufferedOutputStream = new BufferedOutputStream(fileOutputStream);
    byte[] arrayOfByte1 = new byte[1024];
    int i = 0;
    while ((i = byteArrayInputStream.read(arrayOfByte1)) != -1)
      bufferedOutputStream.write(arrayOfByte1, 0, i);
    licenseError = LicenseError.OK;
  } catch (FileNotFoundException fileNotFoundException) {
    licenseError = LicenseError.FILE_WRITE_ERROR;
  } catch (IOException iOException) {
    licenseError = LicenseError.FILE_WRITE_ERROR;
  } finally {
    try {
      if (bufferedOutputStream != null)
        bufferedOutputStream.close();
      if (fileOutputStream != null)
        fileOutputStream.close();
    } catch (IOException iOException) {
      licenseError = LicenseError.FILE_WRITE_ERROR;
    }
  }
  return licenseError;
}
```

However, the check can be bypassed with forward slashes (i.e., ../). The attacker can use path traversal in the license file name to upload an attacker-controlled file to any location on the SMS host. For example, the attacker can upload a reverse shell TCP payload, save it as <SMS_DIR>\ping.exe, and then invoke com.keysight.tentacle.config.SensorConfigurer.sensorPing() (via /server/service/sensorConfigServiceHttpInvoker) to execute the payload, achieving unauthenticated RCE.

The sensorPing() method executes the attacker-supplied ping.exe instead of

```
  public List<String> sensorPing(String paramString) {
    LinkedList<String> linkedList = new LinkedList();
    String str = "";
    try {
      Process process = Runtime.getRuntime().exec("ping " + paramString);
<...snip...>
```

CVE-2022-38130 - smsRestoreDatabaseZip UNC Path RCE (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

The com.keysight.tentacle.config.ResourceManager.smsRestoreDatabaseZip() method is used to restore the HSQLDB database used in SMS. It takes the path of the zipped database file as the single parameter. An unauthenticated, remote attacker can specify an UNC path for the database file (i.e., \\<attacker-host>\sms\<attacker-db.zip>), effectively controlling the content of the database to be restored.

An HSQLDB database includes a script file containing SQL statements to be executed to make up the database. During method execution, the SQL statements in the script file are executed. The attacker can put arbitrary SQL statements in the script to cause them to be executed.

For example, since HSQLDB can call Java static methods, the attacker can use the following SQL statements to load an attacker-controlled DLL into the process executing the script file, achieving unauthenticated RCE.

Solution

Apply the vendor-supplied patch.

Disclosure Timeline

July 4, 2022 - Tenable discloses issues to vendor.
July 5, 2022 - Vendor acknowledges disclosure.
August 10, 2022 - Tenable notices issues have been patched and proceeds with public disclosure.

that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2022-38129
CVE-2022-38130
Tenable Advisory ID: TRA-2022-28
CVSSv3 Base / Temporal Score: 9.8 / 9.1
CVSSv3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: Keysight Technologies Sensor Management Server v2.4.0
Risk Factor: Critical

Advisory Timeline

August 10, 2022 - Initial release.

tenable

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status