# Security Advisory 04122023-001

## CVE-2022-3602
## CVE-2022-3786

## Initial Publication Date: April 12, 2023

Vulnerability Details:

Vulnerability Note VU#794340

- Two buffer overflow vulnerabilities were discovered in OpenSSL versions 3.0.0 through 3.0.6. These vulnerabilities were introduced in version 3.0.0 with the inclusion of support for punycode email address parsing for X.509 certificates. OpenSSL's assessment of the severity of the vulnerabilities has reduced from CRITICAL to HIGH, and OpenSSL 3.0.7 addresses the issues.

CVE-2022-3602

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).
- CVVS Version 3.X Score: 7.5 High

CVE-2022-3786

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.
- CVVS Version 3.X Score: 7.5 High

**Summary**

After evaluation of all MultiTech products and services, it is determined MultiTech does not use OpenSSL 3.0.0 to 3.0.6 decodes in any of its products and services and are not affected by this vulnerability.

**Customer Action Plan**

No action required.

Subscribe to MultiTech Security Alerts and Notifications for updates on this and other security-related issues.

https://info.multitech.com/acton/form/27728/000e:d-0001/1/-/-/-/-/index.htm

### Additional Information

If you have any questions regarding this Security Advisory, please contact your MultiTech sales representative or visit the technical resources listed below:

**World Headquarters – USA**
+1 (763) 785-3500 | sales@multitech.com

**EMEA Headquarters – UK**
+(44) 118 959 7774 | sales@multitech.co.uk

**MultiTech Security Advisories**
www.multitech.com/landing-pages/security
MultiTech monitors industry news and announcements to identify security issues that may impact our devices and operating systems and strives to provide the information and tools to keep your deployments secure and online.

**MultiTech Developer Resources**
www.multitech.net
An open environment where you can ask development related questions and hear back from MultiTech engineering or a member of this community.

**Knowledge Base**
http://www.multitech.com/kb.go
Immediate access to support information and resolutions for all MultiTech products.

**MultiTech Support Portal**
support.multitech.com
Create an account and submit a support case directly to our technical support team.

**MultiTech Website**
www.multitech.com

**Trademarks and Registered Trademarks**
MultiTech and the MultiTech logo are registered trademarks of Multi-Tech Systems, Inc. All other trademarks or registered trademarks are the property of their respective owners.

### Revision History

| Version | Author | Date | Change Description |
|---|---|---|---|
| -001 | DT | 04/12/2023 | Published version |