CERT-EU Security Advisory 2018-006

Remote Code Execution Vulnerability in Exim

March 07, 2018 — v1.0

History:

- *07/03/2018 — v1.0: Initial publication*

Summary

On February 05, 2018, **Devcore Security Consulting** discovered a buffer overflow vulnerability in the base64 decode function of **Exim** message transfer agent [1]. On March 06, 2018, Exim released a security advisory about the issue [2], confirming potential remote code execution that could be triggered by sending a handcrafted message. The issue has been fixed in version 4.90.1 of Exim and no alternative mitigation is known.

Technical Details

The vulnerability received the following CVE number: CVE-2018-6789 [3].

The vulnerability is due to a calculation mistake of decode buffer length in the base64 decode function of Exim. It can be exploited by sending an invalid base64 string to the function. If the string is larger than the buffer, Exim will consume more bytes than the allocated buffer, allowing overwrites of critical data. As the bytes are controllable, the flaw may potentially be exploited for remote code execution.

Products Affected

All versions of **Exim** before 4.90.1 are affected by the vulnerability.

Recommendations

As there is no mitigation known for this vulnerability, is it highly recommended to update Exim to version 4.90.1.

References

[1] https://devco.re/blog/2018/03/06/exim-off-by-one-RCE-exploiting-CVE-2018-6789-en/

[2] https://exim.org/static/doc/security/CVE-2018-6789.txt

[3] https://nvd.nist.gov/vuln/detail/CVE-2018-6789