Title

python stdlib "ipaddress" - Improper Input Validation of octal literals in python 3.8.0 thru v3.10 results in indeterminate SSRF & RFI vulnerabilities. -- "ipaddress leading zeros in IPv4 address"

CVE ID

CVE-2021-29921

CVSS Score

9.8 CRITICAL

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Internal ID

SICK-2021-014

Vendor

python

Product

ipaddress stdlib

Product Versions

3.8.0 thru v3.10

Vulnerability Details

Improper input validation of octal strings in Python 3.8.0 thru v3.10 stdlib ipaddress allows unauthenticated remote attackers to perform indeterminate SSRF, RFI, and LFI attacks on many programs that rely on Python stdlib ipaddress. IP address octects are left stripped instead of evaluated as valid IP addresses. For example, an attacker submitting an IP address to a web application that relies on stdlib ipaddress, could cause SSRF via inputting octal input data; An attacker can submit exploitable IP addresses if the octet is 3 digits, with the minimum exploitable octect being 08 (Denial of Service) and the maximum exploitable octet is 099. For example, an attacker can submit 010.8.8.8, which is 8.8.8.8, yet Python ipaddress builtin will evaluate this as 10.8.8.8.

Vendor Response

Currently unpatched - due to be addressed in next release.

Proof of Concept

Vulnerability added in python3.8

python/cpython#12577

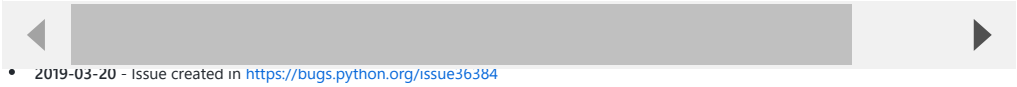
Documentated to be vulnerable in the changelog:

https://github.com/python/cpython/blob/63298930fb531ba2bb4f23bc3b915dbf1e17e9e1/Misc/NEWS.d/3.8.0a4.rst

Stop rejecting IPv4 octets for being ambiguously octal. Leading zeros are ignored, and no longer are assumed to specify octal octets. Octets are always decimal numbers. Octets must still be no more than three digits, including leading zeroes.

```
#!/usr/bin/env python
# Authors:      sickcodes, Victor Viale
# License:      GPLv3+
# Reference:    https://docs.python.org/3.10/library/ipaddress.html#ipaddress.IPv4Address

# Leading zeroes are tolerated only for values less than 8 (as there is no ambiguity between the decimal and octal interpretations of

import subprocess
import ipaddress

SUSPECT = '010.8.8.8'

print(ipaddress.ip_network(SUSPECT, strict=True))
```

```
BAD_IP = ipaddress.ip_address(SUSPECT)

print('http://'+str(BAD_IP))

print(str(subprocess.check_output("ping -W3 -v -c1 "+str(SUSPECT), shell=True, universal_newlines=True).strip()))

print(str(subprocess.check_output("ping -W3 -v -c1 "+str(BAD_IP), shell=True, universal_newlines=True).strip()))
```



- **2019-03-20** - Issue created in https://bugs.python.org/issue36384
- **2021-03-29** - Researchers discover vulnerability
- **2021-03-29** - Vendor notified
- **2021-03-29** - CVE requested
- **2021-04-30** - CVE Assigned CVE-2021-29921 https://bugs.python.org/issue36384#msg392423
- **2021-04-30** - CVE published

Links

https://github.com/python/cpython

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-014.md

https://sick.codes/sick-2021-014

https://python-security.readthedocs.io/vuln/ipaddress-ipv4-leading-zeros.html

https://bugs.python.org/issue36384

https://docs.python.org/3/library/ipaddress.html

python/cpython#12577

python/cpython#25099

https://github.com/python/cpython/blob/63298930fb531ba2bb4f23bc3b915dbf1e17e9e1/Misc/NEWS.d/3.8.0a4.rst

Researchers

Joel Croteau: https://github.com/TV4Fun

Victor Viale: https://github.com/koroeskohr || https://twitter.com/koroeskohr

Sick Codes: https://github.com/sickcodes || https://twitter.com/sickcodes

Kelly Kaoudis: https://github.com/kaoudis || https://twitter.com/kaoudis

John Jackson https://www.twitter.com/johnjhacking

Nick Sahler: https://github.com/nicksahler || https://twitter.com/tensor_bodega

Christian Heimes: https://github.com/tiran

Victor Stinner: https://github.com/vstinner

CVE Links

https://sick.codes/sick-2021-014

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29921

https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-29921