Microsoft Azure DevOps Server 2020.0.1 Cross Site Scripting

Authored by M. Li | Site sec-consult.com

Posted Apr 14, 2021

Microsoft Azure DevOps Server version 2020.0.1 suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2021-28459
SHA-256 | 2865bdfc703b7d0f9e4183f21398f57ed28f9364149b790650846f15f2d1f767 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

````
SEC Consult Vulnerability Lab Security Advisory < 20210414-0 >
=======================================================================
              title: Reflected cross-site scripting
            product: Microsoft Azure DevOps Server
 vulnerable version: 2020.0.1
      fixed version: 2020.0.1 Patch 2
         CVE number: CVE-2021-28459
             impact: medium
           homepage: https://azure.microsoft.com/en-us/services/devops/server/
              found: 2021-03-03
                 by: M. Li (Office Munich)
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult, an Atos company
                     Europe | Asia | North America

                     https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"What is Azure DevOps Server?
Collaborative software development tools for the entire team

Previously known as Team Foundation Server (TFS), Azure DevOps Server is a set
of collaborative software development tools, hosted on-premises.
Azure DevOps Server integrates with your existing IDE or editor, enabling
your
cross-functional team to work effectively on projects of all sizes."

Source: https://azure.microsoft.com/en-us/services/devops/server/


Business recommendation:
------------------------
SEC Consult recommends upgrading to the latest available version which patches
the security issues.

An in-depth security analysis performed by security professionals is advised,
as the software may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
1) Reflected cross-site scripting
The process template function with the collection settings allows uploading of
a zip file, from which the name of the template is taken and returned to the
browser. This variable is not sanitized, leading to a reflected cross-site
scripting vulnerability.


Proof of concept:
-----------------
1) Reflected cross-site scripting
An authenticated user with privileges to upload project files can access the
Collection Settings of one project. Under the Process function, it is possible
to upload a process template in form of a zip file, which can be obtained
by
downloading an existing template. According to the template structure, the
ProcessTemplate.xml file should contain a name, in which the XSS payload is
injected as below:

```
<ProcessTemplate>
  <metadata>
    <name>XSS here: <img src=x onerror=alert(document.URL)></name>
    <description>This template is flexible and will work great</description>
    <version type="aa12a345-00a0-1f11-ba00-b12345b12345" major="1" minor="0" />
    <plugins>
```

Soon after the upload, a message is returned to the user, stating the process
template has been renamed to the malicious one with the XSS payload. At this
point, the injected JavaScript will get executed, showing a pop-up window
with
the URL in this case.

In reality, an attacker might send a malicious zip file to administrators
and
trick them into uploading it, thus achieving to compromise their account.


Vulnerable / tested versions:
-----------------------------
The following version has been tested, which was the most recent one at the
time of the test:
- 2020.0.1


Vendor contact timeline:
------------------------
2021-03-08: Contacting vendor through MSRC portal, case number 64141 is auto-assigned.
2021-03-09: Vendor informed that the investigation be started.
2021-04-01: Vendor informed that a fix has been completed and will be released as part
            of April Patch Tuesday. CVE-2021-28459 has been assigned to the issue.
2021-04-13: Vendor released the patch.
2021-04-14: Public release of the security advisory.


Solution:
---------
The patch is available at:
https://docs.microsoft.com/en-us/azure/devops/server/release-notes/azuredevops2020?view=azure-
devops&branch=releasenotes%2Fmarchpatch#azure-devops-server-202001-patch-2-release-date-march-9-202


Workaround:
-----------
None


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America
````

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	157 files
Ubuntu	76 files
LiquidWorm	23 files
Debian	21 files
nu11secur1ty	11 files
malvuln	11 files
Gentoo	9 files
Google Security Research	8 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

```
About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF M. Li / @2021
```

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Login or Register to add favorites

packet storm

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed