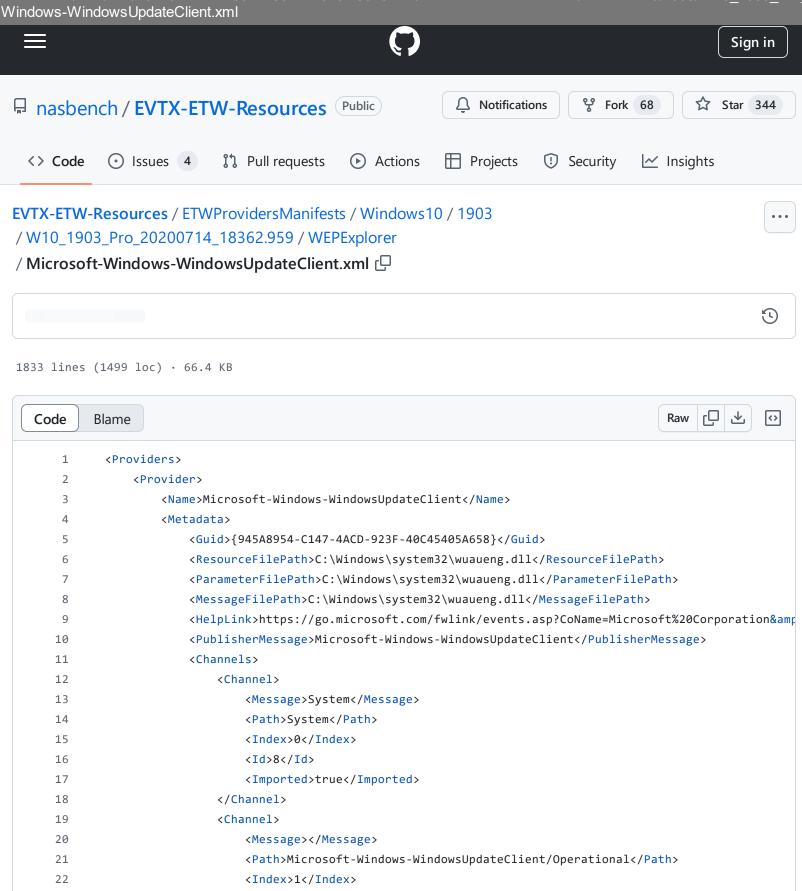
23

24

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10 1903 Pro



<Id>16</Id>

<Imported>false</Imported>

Windows-WindowsUpdateClient.xml

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources · Github - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETWResources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10 1903 Pro 3

```
26
                        <Channel>
27
                             <Message></Message>
28
                             <Path>Microsoft-Windows-WindowsUpdateClient/Analytic</Path>
29
                            <Index>2</Index>
30
                             <Id>17</Id>
31
                            <Imported>false</Imported>
32
                        </Channel>
33
                    </Channels>
34
                    <Levels>
35
                        <Level>
36
                            <Message>Error</Message>
37
                            <Name>win:Error</Name>
38
                             <Value>2</Value>
39
                        </Level>
40
                        <Level>
41
                            <Message>Warning</Message>
42
                            <Name>win:Warning</Name>
43
                            <Value>3</Value>
44
                        </Level>
45
                        <Level>
46
                             <Message>Information</Message>
47
                            <Name>win:Informational</Name>
48
                            <Value>4</Value>
49
                        </Level>
50
                    </Levels>
51
                    <Tasks>
52
                        <Task>
53
                             <Message>Windows Update Agent</Message>
54
                            <Name>Agent</Name>
55
                            <Value>1</Value>
56
                        </Task>
57
                        <Task>
58
                             <Message>Automatic Updates</Message>
59
                             <Name>AU</Name>
                            <Value>2</Value>
60
61
                        </Task>
62
                    </Tasks>
63
                    <Opcodes>
64
                        <Opcode>
65
                             <Message>Info</Message>
66
                            <Name>win:Info</Name>
67
                             <Value>0</Value>
68
                            <Task>0</Task>
69
                        </Opcode>
                        70
```

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_XUINDOWSUpdateClient.xml

```
<message>Start</message>
72
                              <Name>win:Start</Name>
 73
                              <Value>1</Value>
 74
                              <Task>0</Task>
 75
                         </Opcode>
 76
                         <Opcode>
 77
                              <Message>Stop</Message>
 78
                              <Name>win:Stop</Name>
 79
                              <Value>2</Value>
 80
                              <Task>0</Task>
 81
                         </Opcode>
 82
                         <Opcode>
 83
                              <Message>SelfUpdate</Message>
 84
                              <Name>selfupdate</Name>
 85
                              <Value>10</Value>
 86
                              <Task>0</Task>
 87
                         </Opcode>
 88
                         <Opcode>
 89
                              <Message>Check for Updates</Message>
 90
                              <Name>detect</Name>
 91
                              <Value>11</Value>
 92
                              <Task>0</Task>
 93
                         </Opcode>
 94
                         <Opcode>
 95
                              <Message>Download</Message>
96
                              <Name>download</Name>
 97
                              <Value>12</Value>
 98
                              <Task>0</Task>
 99
                         </Opcode>
100
                         <Opcode>
101
                              <Message>Installation</Message>
102
                              <Name>install</Name>
                              <Value>13</Value>
103
                              <Task>0</Task>
104
105
                         </Opcode>
106
                         <Opcode>
107
                              <Message>Uninstallation</Message>
108
                              <Name>uninstall</Name>
                              <Value>14</Value>
109
                              <Task>0</Task>
110
111
                         </Opcode>
                         <Opcode>
112
113
                              <Message>Reboot</Message>
114
                              <Name>reboot</Name>
                              <Value>15</Value>
115
```

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

117	dateClient.xml 0pcode		

Windows-WindowsUpd Resources · GitHub - 3	ersManifests/Windows10/1 ateClient.xml at f1b010ce0e 1/10/2024 16:00 https://githuk e0ee1b71e3024180de1a3e67 teClient.xml	ee1b71e3024180de1a3e67 b.com/nasbench/EVTX-ETV	7f99701fe4 · nasbench/EVT /√-	X-ETW-

Windows-WindowsUpo Resources · GitHub - 3	dateClient.xml at f1b010ce0 31/10/2024 16:00 https://githu ce0ee1b71e3024180de1a3e6	ee1b71e3024180de1a3e6 b.com/nasbench/EVTX-ET	0714_18362.959/WEPExplore 7f99701fe4 · nasbench/EVTX W- //anifests/Windows10/1903/W1	-ETW-

Windows-WindowsUpda Resources · GitHub - 3	ateClient.xml at f1b010ce0e 1/10/2024 16:00 https://github e0ee1b71e3024180de1a3e67	e1b71e3024180de1a3e67 b.com/nasbench/EVTX-ETW	714_18362.959/WEPExplorer f 99701fe4 · nasbench/EVTX- V- lanifests/Windows10/1903/W10	ETW-

Windows-WindowsUp Resources · GitHub	vidersManifests/Windows10 pdateClient.xml at f1b010ce - 31/10/2024 16:00 https://gitl 0ce0ee1b71e3024180de1a3e dateClient.xml	e <mark>0ee1b71e3024180de1a</mark> hub.com/nasbench/EVT)	a3e67f99701fe4 · nasbe X-ETW-	nch/EVTX-ETW-

Resources/ETWProvidersMan Windows-WindowsUpdateClie Resources · GitHub - 31/10/202 Resources/blob/f1b010ce0ee1b7 Windows-WindowsUpdateClient.	nt.xml at f1b010ce0ee1b71e 24 16:00 https://github.com/na 1e3024180de1a3e67f99701fe	3024180de1a3e67f99701fe 4 sbench/EVTX-ETW-	4 · nasbench/EVTX-ET	W-

Windows-WindowsUpdate C Resources · GitHub - 31/10	Client.xml at f1b010ce0ee //2024 16:00 https://github.c e1b71e3024180de1a3e67f9	1b71e3024180de1a3e67f om/nasbench/EVTX-ETW	14_18362.959/WEPExplorer 99701fe4 · nasbench/EVTX- - nifests/Windows10/1903/W10	ETW-

Windows-Windows Resources · GitHu	rovidersManifests/WindowsUpdateClient.xml at f1b0 ub - 31/10/2024 16:00 https: 010ce0ee1b71e3024180de UpdateClient.xml	10ce0ee1b71e302418 0 ://github.com/nasbench/	0de1a3e67f99701fe4 · n /EVTX-ETW-	nasbench/EVTX-ET	W-

Windows-WindowsUp Resources · GitHub ·	odateClient.xml at f1b010ce - 31/10/2024 16:00 https://gith 0ce0ee1b71e3024180de1a3e	0ee1b71e3024180de1a3e ub.com/nasbench/EVTX-E	200714_18362.959/WEPExplore e67f99701fe4 · nasbench/EVT ETW- rsManifests/Windows10/1903/V	X-ETW-

Windows-WindowsUpo Resources · GitHub - 3	lateClient.xml at f1b010ce0 31/10/2024 16:00 https://githเ :e0ee1b71e3024180de1a3e6	Dee1b71e3024180de1a3 ub.com/nasbench/EVTX-l	200714_18362.959/WEPExpe67f99701fe4 · nasbench/E ETW- ersManifests/Windows10/190	VTX-ETW-

Windows-WindowsUpd Resources · GitHub - 3	ateClient.xml at f1b010ce0 31/10/2024 16:00 https://githu e0ee1b71e3024180de1a3e6	ee1b71e3024180de1a3e6 b.com/nasbench/EVTX-ET	00714_18362.959/WEPExplo 67f99701fe4 · nasbench/EV W- Manifests/Windows10/1903/\	TX-ETW-

Windows-Window Resources · Gith Resources/blob/f1	ProvidersManifests/V wsUpdateClient.xml a Hub - 31/10/2024 16:00 lb010ce0ee1b71e3024 vsUpdateClient.xml	t f1b010ce0ee1b71 https://github.com/n	e <mark>3024180de1a3e67f</mark> asbench/EVTX-ETW	f99701fe4 · nasbencl /-	n/EVTX-ETW-

Windows-WindowsUp Resources · GitHub -	idersManifests/Windows10 odateClient.xml at f1b010co 31/10/2024 16:00 https://gitl 0ce0ee1b71e3024180de1a3odateClient.xml	e <mark>0ee1b71e3024180de1</mark> a hub.com/nasbench/EVT	a3e67f99701fe4 · nasben X-ETW-	ch/EVTX-ETW-

Windows-WindowsU Resources · GitHub	pdateClient.xml at f1b010ce - 31/10/2024 16:00 https://gith 0ce0ee1b71e3024180de1a3e	0ee1b71e3024180de1a3 ub.com/nasbench/EVTX-E	200714_18362.959/WEPExploe67f99701fe4 · nasbench/EV ETW- rsManifests/Windows10/1903/	TX-ETW-

Windows-Windows Resources · GitHu	UpdateClient.xml at f1b010 b - 31/10/2024 16:00 https://o 010ce0ee1b71e3024180de1a	oce0ee1b71e3024180de1a github.com/nasbench/EVT	20200714_18362.959/WEPE a3e67f99701fe4 · nasbench X-ETW- dersManifests/Windows10/19	n/EVTX-ETW-

Resources/ETWProvidersManif Windows-WindowsUpdateClient Resources · GitHub - 31/10/2024 Resources/blob/f1b010ce0ee1b71 Windows-WindowsUpdateClient.xi	. xml at f1b010ce0ee1b71e - 16:00 https://github.com/na e3024180de1a3e67f99701f	e3024180de1a3e67f99701f asbench/EVTX-ETW-	fe4 · nasbench/EVTX-E	TW-

Windows-WindowsUpdateClient.: Resources · GitHub - 31/10/2024	xml at f1b010ce0ee1b71e302418 16:00 https://github.com/nasbench :3024180de1a3e67f99701fe4/ETW	Pro_20200714_18362.959/WEPExplorer/logoe1a3e67f99701fe4 · nasbench/EVTX-En/EVTX-ETW- ProvidersManifests/Windows10/1903/W10	TW-

Windows-WindowsUpdateClient.xml a Resources · GitHub - 31/10/2024 16:00	Windows10/1903/W10_1903_Pro_2020071 at f1b010ce0ee1b71e3024180de1a3e67f9 0 https://github.com/nasbench/EVTX-ETW- 4180de1a3e67f99701fe4/ETWProvidersMar	9701fe4 · nasbench/EVTX-ETW-

Windows-WindowsUpdateClient. Resources · GitHub - 31/10/2024	xml at f1b010ce0ee1b71e30241 16:00 https://github.com/nasbence3024180de1a3e67f99701fe4/ETV	S_Pro_20200714_18362.959/WEPExpl 80de1a3e67f99701fe4 · nasbench/EV h/EVTX-ETW- VProvidersManifests/Windows10/1903	VTX-ETW-

Resources/ETWProvidersManife Windows-WindowsUpdateClient. Resources · GitHub - 31/10/2024 Resources/blob/f1b010ce0ee1b71e Windows-WindowsUpdateClient.xn	xml at f1b010ce0ee1b71e30 16:00 https://github.com/nasb e3024180de1a3e67f99701fe4/	24180de1a3e67f99701fe4 · ench/EVTX-ETW-	nasbench/EVTX-ETW	-

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft	
Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-	
Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_ProvidersWindowsUpdateClient.xml	D _.
	_

Resources/ETWProvidersManife Windows-WindowsUpdateClient. Resources · GitHub - 31/10/2024 Resources/blob/f1b010ce0ee1b71e Windows-WindowsUpdateClient.xn	xml at f1b010ce0ee1b71e3024 16:00 https://github.com/nasben e3024180de1a3e67f99701fe4/ET	180de1a3e67f99701fe4 · nasb nch/EVTX-ETW-	ench/EVTX-ETW-

Resources/ETWProvidersMai Windows-WindowsUpdateClie Resources · GitHub - 31/10/20 Resources/blob/f1b010ce0ee1b Windows-WindowsUpdateClient	nt.xml at f1b010ce0ee1b7′ 24 16:00 https://github.com/ 71e3024180de1a3e67f9970′	le3024180de1a3e67f99701f nasbench/EVTX-ETW-	e4 · nasbench/EVTX-ET	W-

Windows-Windows Resources · GitHu	rovidersManifests/WindosUpdateClient.xml at f1b ub - 31/10/2024 16:00 https 010ce0ee1b71e3024180d UpdateClient.xml	010ce0ee1b71e30241 s://github.com/nasbend	80de1a3e67f99701fe4 :h/EVTX-ETW-	· nasbench/EVTX-E	TW-

Resources/ETWProvidersMan Windows-WindowsUpdateClier Resources · GitHub - 31/10/202 Resources/blob/f1b010ce0ee1b7 Windows-WindowsUpdateClient.	nt.xml at f1b010ce0ee1b71e30 4 16:00 https://github.com/nast 1e3024180de1a3e67f99701fe4/)24180de1a3e67f99701fe4 ·	nasbench/EVTX-ETW	_

Windows-WindowsUpdateClient.x Resources · GitHub - 31/10/2024 1	t ml at f1b010ce0ee1b71e3024180de l6:00 https://github.com/nasbench/EV 3024180de1a3e67f99701fe4/ETWPro	o_20200714_18362.959/WEPExplorer/Meta3e67f99701fe4 · nasbench/EVTX-ET TX-ETW- ovidersManifests/Windows10/1903/W10_	W-

Windows-WindowsUpdateClient. Resources · GitHub - 31/10/2024	. xml at f1b010ce0ee1b71e302418 16:00 https://github.com/nasbench e3024180de1a3e67f99701fe4/ETW	_Pro_20200714_18362.959/WEPExplore 30de1a3e67f99701fe4 · nasbench/EVTX h/EVTX-ETW- VProvidersManifests/Windows10/1903/W	C-ETW-

Windows-WindowsU Resources · GitHub	vidersManifests/Windows IpdateClient.xml at f1b010 - 31/10/2024 16:00 https://g 10ce0ee1b71e3024180de1a pdateClient.xml	i <mark>ce0ee1b71e3024180de1</mark> github.com/nasbench/EVT	a3e67f99701fe4 · nasber X-ETW-	nch/EVTX-ETW-

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_X Windows-WindowsUpdateClient.xml

```
1426
                         <Channel>System</Channel>
1427
                         <Level>Information</Level>
1428
                         <Task>Windows Update Agent</Task>
1429
                         <Opcode>Revert</Opcode>
1430
                         <Keyword>Success Revert</Keyword>
1431
                         <Message><![CDATA[
         Revert Successful: Windows successfully reverted the following update: %1]]></Message>
1432
1433
                         <Template><![CDATA[
1434
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1435
           <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1436
           <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
           <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1437
1438
           <data name="serviceGuid" inType="win:GUID" outType="xs:GUID"/>
1439
         </template>
1440
         ]]></Template>
1441
                     </Event>
1442
                     <Event>
1443
                         <Id>213</Id>
1444
```

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_; Windows-WindowsUpdateClient.xml

```
<cnannel>System</cnannel>
1446
                         <Level>Error</Level>
1447
                         <Task>Windows Update Agent</Task>
1448
                         <Opcode>Revert</Opcode>
1449
                         <Keyword>Failure Revert</Keyword>
1450
                          <Message><![CDATA[
         Revert Failure: Windows failed to revert the following update with error %1: %2]]></Message>
1451
1452
                         <Template><![CDATA[
1453
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
           <data name="errorCode" inType="win:HexInt32" outType="win:HexInt32"/>
1454
1455
           <data name="updatelist" inType="win:UnicodeString" outType="xs:string"/>
1456
           <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
           <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1457
1458
         </template>
         ]]></Template>
1459
1460
                      </Event>
1461
                      <Event>
                         <Id>214</Id>
1462
1463
                         <Version>0</Version>
                         <Channel>System</Channel>
1464
1465
                         <Level>Information</Level>
1466
                         <Task>Windows Update Agent</Task>
1467
                         <Opcode>Revert</Opcode>
1468
                         <Keyword>Started Revert</Keyword>
1469
                          <Message><![CDATA[
         Revert Started: Windows has started reverting the following update: %1]]></Message>
1470
1471
                         <Template><![CDATA[
1472
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
           <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1473
1474
           <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1475
           <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1476
         </template>
1477
         ]]></Template>
1478
                      </Event>
1479
                      <Fvent>
1480
                         <Id>215</Id>
1481
                         <Version>0</Version>
                          <Channel>System</Channel>
1482
1483
                         <Level>Information</Level>
1484
                         <Task>Windows Update Agent</Task>
1485
                         <Opcode>Uninstallation</Opcode>
1486
                         <Keyword>Started Uninstallation</Keyword>
1487
                         <Message><![CDATA[
1488
         Uninstallation started: Windows has started uninstallnig the following update: %1]]></Message>
1489
                         <Template><![CDATA[
```

Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_XUINDOWSUpdateClient.xml

```
<data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1491
           <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1492
           <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1493
1494
         </template>
         ]]></Template>
1495
1496
                     </Event>
1497
                 </EventMetadata>
1498
             </Provider>
1499
         </Providers>
```