

Distributed Malware Exploiting Vulnerable Innorix: Andariel

eastston :: 2/15/2023



The AhnLab Security Emergency response Center (ASEC) analysis team confirmed the distribution of malicious codes targeting users of the vulnerable version of Innorix Agent. The secured malicious code tries to connect to the C&C server through a backdoor.

□ 개요

- o 이노릭스 INNORIX Agent*에 대한 파일 다운로드 및 실행 취약점을 해결한 보안 업데이트 발표
- * INNORIX Agent : 파일 전송 솔루션 클라이언트 프로그램
- o 공격자는 해당 취약점을 악용하여 악성코드 감염 등의 피해를 발생시킬 수 있으므로, 해당 제품을 사용하는 이용자들은 최신 버전으로 업데이트 권고

□ 설명

- o INNORIX Agent*에서 발생하는 파일 다운로드 및 실행 취약점

□ 영향 받는 제품 및 버전

- o INNORIX Agent 9.2.18.450 및 이전 버전

□ 해결 방안

- o 취약한 버전의 INNORIX Agent가 설치되어 있는 경우 삭제 조치
- [제어판]-[프로그램]-[프로그램 및 기능]에서 INNORIX Agent의 버전 확인 후 제거 클릭

프로그램 제거 또는 변경
프로그램을 제거하려면 목록에서 선택한 후 (제거), (변경) 또는 (복구)를 클릭하십시오.

이름	게시자	설치 날짜	크기	버전
INNORIX Agent	INNORIX	2022-05-13		9.2.18.334
IntelliJ IDEA Community Edition 2021.3.3	JetBrains s.r.o.	2022-04-01		213.7172.25
Java 8 Update 321 (64-bit)	Oracle Corporation	2022-03-11	127MB	8.0.3210.7
Java(TM) SE Development Kit 11.0.14 (64-bit)	Oracle Corporation	2022-04-01	255MB	11.0.14.0
Microsoft Edge	Microsoft Corporation	2022-05-06		101.0.1210.39
Microsoft OneDrive	Microsoft Corporation	2022-05-02	238MB	22.077.0410.0007

- o 아래 URL에서 최신 버전을 다운로드 받아 압축 해제 후 설치
- URL : http://dist.innorix.com:8080/download/INNORIX-Agent-Lastest_Version.zip

□ 기타 문의사항



- o 이노릭스 : 02) 557-2757
- o 한국인터넷진흥원 인터넷침해대응센터: 국번없이 118




□ 작성 : 취약점분석팀

출처 사이트 : https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=66748

[Figure 1] Korea Internet & Security Agency Vulnerability Security Update Notice [1]

The Innorix Agent program that was exploited for distribution is a file transfer solution client program. The Korea Internet & Security Agency (KISA) [1] published information about the vulnerability and recommended a security update to INNORIX Agent 9.2.18.450 and 9.2.18.418 corresponding to previous versions. confirmed with

Target Type	File Name	File Size	File Path ⓘ
Current	 innorixas.exe	8.17 MB	%SystemDrive%\innorix_agent\innorixas.exe
Target	 msdes.exe.irx	40.5 KB	%SystemDrive%\users\%ASD%\msdes.exe.irx

Process	Module	Target	Data
 innorixas.exe	N/A	N/A	 msdes.exe.irx
 innorixas.exe	N/A	N/A	http://4.246.144.112/update.exe

[Figure 2] ASD infrastructure detection log

The detected backdoor attempts to connect to the C&C server. Its main function is to collect and transmit information on the user's PC, as well as to capture screens and create and execute files.

CMDLine

```
schtasks /delete /tn "ahnlab\asdclient"
schtasks /create /tn "ahnlab\asdclient" /tr "c:\users\%ASD%\msdes.exe" /sc daily /st 09:05:20 /ru qwerty
```

[Figure 3] ASD infrastructure detection report

The confirmed backdoor was a form with two external appearances, the form initially discovered was confirmed to be developed in C/C++, and the recently detected sample was produced in .Net. There is no difference in function between the two forms, and in some detection reports, it was confirmed that when registering malicious code in the task scheduler, it uses the method of concealment by using the company name (AhnLab) in the task name.

```

do
{
  if ( !v5 )
    _report_rangecheckfailure(a1, a2, a3, a2);
  v18[v3++] = 0;
  v5 = (unsigned __int64)v3 < 16;
}
while ( v3 < 16 );
v6 = (int)a3;
if ( (int)a3 > 0 )
{
  v7 = a1 - (_QWORD)a2;
  do
  {
    v8 = 8i64;
    do
    {
      v9 = 15i64;
      v10 = (unsigned __int8)v18[15] >> 7;
      do
      {
        v18[v9] = __ROL1__(v18[v9 - 1], 1);
        --v9;
      }
      while ( v9 > 0 );
      v11 = 2 * v18[0];
      v18[0] *= 2;
      if ( v10 )
      {
        v13 = 0;
        v14 = 0i64;
        do
        {
          v15 = v13++ ^ v18[v14] ^ byte_140020900[v14];
          v18[v14++] = v15;
        }
        while ( v13 < 16 );
        v12 = v18[0];
      }
      else
      {
        v12 = v11 | 1;
        v18[0] = v12;
      }
      --v8;
    }
    while ( v8 );
    LOBYTE(v3) = v12 ^ v4[v7];
    *v4++ = v3;
    --v6;
  }
  while ( v6 );
}
return v3;

```

[Figure 4] Encoding and decoding routines

This malicious code classified as a backdoor uses data using the routine shown in [Figure 4] when receiving data, and transmits data using the same method when sending data. Data is encrypted and transmitted through encoding and decoding routines, bypassing packet-level monitoring, and can be seen as a feature of Andardoor based on its diagnosis. The key value is 74615104773254458995125212023273 , which is the same as the XOR key value specified in the CISA report [\[2\]](#) written in 2017 .

Recently, the form of distribution as a vulnerability in software has been confirmed, so corporate users and general users need to pay special attention. Vulnerable versions of software should be managed for use after updating.

[File Diagnosis]

- Backdoor/Win.Andardoor.R558252
- Backdoor/Win.Andardoor.C5381120
- Backdoor/Win.Andardoor.C5382662

- Backdoor/Win.Andardoor.C5382103
- Backdoor/Win.Andardoor.C5382101

[IOC]

- bcac28919fa33704a01d7a9e5e3ddf3f
- 1ffccc23fef2964e9b1747098c19d956
- 9112efb49cae021abebd3e9a564e6ca4
- 0a09b7f2317b3d5f057180be6b6d0755
- 0211a3160cc5871cbcd4e5514449162b
- ac0ada011f1544aa3a1cf27a26f2e288
- c892c60817e6399f939987bd2bf5dee0
- 6dd579cfa0cb4a0eb79414de6fc1d147
- 88a7c84ac7f7ed310b5ee791ec8bd6c5
- e5410abaaac69c88db84ab3d0e9485ac
- 4.246.144[.]112:443
- 139.177.190[.]243:443
- 27.102.107[.]224:5443
- 27.102.107[.]234:8443
- 27.102.113[.]88:5443
- 27.102.113[.]88:21
- 109.248.150[.]179:443

[References]

- 1) <https://knvd.krcert.or.kr/detailSecNo.do?IDX=5622>
- 2) https://www.cisa.gov/uscert/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF