

[NT] Bypassing Pedestal Software Integrity Protection Driver (Time Vulnerability)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0030.html>

From: support@securiteam.com

Date: 12/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: 8 Dec 2002 23:32:26 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Bypassing Pedestal Software Integrity Protection Driver (Time Vulnerability)

SUMMARY

The IPD is an Open Source device driver designed to prohibit the installation of new services and drivers and to protect existing drivers from tampering. It installs on Windows NT and Windows 2000 computers. [...] This driver was created to provide protection against Rootkit installation by attempting to block any new kernel code from being installed and executed. This will help to prevent Trojan hiding from integrity checking programs such as Intact.

To give administrator ability to uninstall IPD, the driver starts protecting the system 20 minutes after being loaded. This is acceptable, because we can assume that right after reboot server can be disconnected from the Internet. Due to this an attacker can move back the clock and bypass the protection mechanism.

DETAILS

Vulnerable systems:

* IPD version 1.2

Securiteam: [NT] Bypassing Pedestal Software Integrity Protection Driver (Time Vulnerability)

Immune systems:

* IPD version 1.3

In order to provide 20 minutes delay on startup, restrictEnabled() function is used. It is called from other functions to check, whether they should be restrictive about various actions (like loading drivers) or not:

```
int restrictEnabled() {
    LARGE_INTEGER curtime, diff;
    KeQuerySystemTime(&curtime);
    diff = RtlLargeIntegerSubtract(curtime, Globals.DRIVERSTARTTIME);

    if (RtlLargeIntegerGreaterThan(diff,
    Globals.RESTRICT_STARTUP_TIMEOUT))
        return 1;
    return 0;
}
```

One can easily circumvent IPD's protection by turning system clock back. (Yes, one must own SeSystemtimePrivilege, but that is not a problem when the attacker has gained privileged access to the system).

Proof-Of-Concept:

00:00 [real admin starts IPD on his server]

```
c:\ipd>ipdinstall.exe start
```

[...]

The driver will engage in 20 minutes.

```
c:\ipd>
```

00:21 [IPD starts protecting the system from inserting drivers]

...

13:13 [a bad hacker comes in to the system]

```
c:\alamakota> time
```

[now he turns the clock 14 hours back]

```
c:\alamakota> w2k_load verybaddrv.sys
```

```
c:\alamakota> time
```

[he restores the original time]

[system is compromised]

Patch:

Jan has contacted Pedestal Software, and they released (on Monday 2/12/2002) a new version (1.3), which fixes this vulnerability. This can be downloaded from IPD home page (see References below).

Postscriptum:

Another IPD vulnerability, was described by crazylord in the last issue of phrack. He showed how to cheat IPD so that it allows writing to /Device/PhysicalMemory (by creating a symlink).

Solution:

Both these vulnerabilities have been fixed in the new version 1.3.

Securiteam: [NT] Bypassing Pedestal Software Integrity Protection Driver (Time Vulnerability)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jkrutkowski@elka.pw.edu.pl>>
Jan K. Rutkowski.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.