Product Security Information

WinVerifyTrust Signature Validation Vulnerability
BOSCH-SI-2024-0702 BT

Overview

WinVerifyTrust Signature Validation CVE-2013-3900 was first published on 10 December 2013, disclosing a remote code execution vulnerability. The vulnerability was found in the mechanism that the WinVerifyTrust function uses to handle Windows Authenticode signature verification for portable executable (PE) files, allowing malicious actors to take advantage of padding a Windows Authenticode signature to hijack a system.

Microsoft has provided an "opt-in" solution to mitigate the vulnerability by enforcing stricter verification. However, Microsoft has decided to stop enforcing it on 29 July 2014 mainly due to issues with installers.

Although Microsoft has rolled back enforcing stricter verification by default, the systems remain at risk. As a result, bad actors have exploited this open vulnerability by installing malware and ransomware. Bosch follows Microsoft's default settings but acknowledges the risk and encourages enforcing the stricter verification behavior for its DIVAR IP all-in-one products.

Affected Products

Bosch DIVAR IP all-in-one 4000 (DIP-44xx)
Bosch DIVAR IP all-in-one 5000 (DIP-52xx)
Bosch DIVAR IP all-in-one 6000 (DIP-64xx)
Bosch DIVAR IP all-in-one 7000 (DIP-72xx)
Bosch DIVAR IP all-in-one 7000 R3 (DIP-73xx)
Bosch DIVAR IP all-in-one 7000 (DIP-74xx)

Technical Details

1.1 Considered Common Vulnerabilities and Exposures (CVE)

CVE-2013-3900 (CVSS v2 Base Score: 7.6 Medium)

1.2 Vulnerability Details

CVE-2013-3900
The WinVerifyTrust function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate PE file digests during Authenticode signature verification, which allows remote attackers to execute arbitrary code via a crafted PE file, aka "WinVerifyTrust Signature Validation Vulnerability."

1.3 References

https://nvd.nist.gov/vuln/detail/CVE-2013-3900
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

Solutions and Mitigations

Opt for stricter verification behavior by enforcing the WinVerifyTrust function to perform strict Windows Authenticode signature verification for PE files. To apply the fix, paste the following text into a text editor such as Notepad. Then save the file using a .reg filename extension, for instance '*AuthenticodeVerification.reg*', and finally double-click on the file to apply it.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"
```

Warning!
The system must be restarted for the changes to take effect. Please save your work and close all applications before rebooting to avoid data loss or interruption. Please also note that the reboot may result in a recording gap for a short period of time.

Notice!
For consistent functionality, compatibility, performance, and security, regularly update the software to the latest approved version throughout the operational life of the device.

Material Lists

Bosch DIVAR IP all-in-one 4000 (DIP-44xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 4000	DIP-4420IG-00N	F.01U.404.040	Management appliance w/o HDD
DIVAR IP all-in-one 4000	DIP-4424IG-2HD	F.01U.404.041	Management appliance 2x4TB
DIVAR IP all-in-one 4000	DIP-4428IG-2HD	F.01U.404.042	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP-442IIG-2HD	F.01U.404.043	Management appliance 2x18TB

Bosch DIVAR IP all-in-one 5000 (DIP-52xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-5240IG-00N	F.01U.361.821	Management Appliance w/o HDD
DIVAR IP all-in-one 5000	DIP-5244IG-4HD	F.01U.362.424	Management Appliance 4x4TB
DIVAR IP all-in-one 5000	DIP-5248IG-4HD	F.01U.362.423	Management Appliance 4x8TB
DIVAR IP all-in-one 5000	DIP-524CIG-4HD	F.01U.362.422	Management Appliance 4x12TB
DIVAR IP all-in-one 5000	DIP-5240GP-00N	F.01U.359.551	Management Appliance GPU wo HD
DIVAR IP all-in-one 5000	DIP-5244GP-4HD	F.01U.359.552	Management Appliance GPU 4x4TB
DIVAR IP all-in-one 5000	DIP-5248GP-4HD	F.01U.359.553	Management Appliance GPU 4x8TB
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4x12TB

DIVAR IP all-in-one 6000 (DIP-64xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 6000	DIP-6440IG-00N	F.01U.404.045	Management appliance 1U w/o HDD
DIVAR IP all-in-one 6000	DIP-6444IG-4HD	F.01U.404.046	Management appliance 1U 4x4TB
DIVAR IP all-in-one 6000	DIP-6448IG-4HD	F.01U.404.047	Management appliance 1U 4x8TB
DIVAR IP all-in-one 6000	DIP-644IIG-4HD	F.01U.404.048	Management appliance 1U 4x18TB

Bosch DIVAR IP all-in-one 7000 (DIP-72xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7280-00N	F.01U.362.591	2U Management Appliance w/o HD
DIVAR IP all-in-one 7000	DIP-7284-8HD	F.01U.362.592	2U Management Appliance 8x4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	2U Management Appliance 8x8TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	2U Management Appliance 8x12TB
DIVAR IP all-in-one 7000	DIP-72G0-00N	F.01U.362.595	3U Management Appliance wo HDD
DIVAR IP all-in-one 7000	DIP-72G8-16HD	F.01U.362.596	3U Management Appliance 16x8TB
DIVAR IP all-in-one 7000	DIP-72GC-16HD	F.01U.362.597	3U Management Appliance 16x12T

Bosch DIVAR IP all-in-one 7000 R3 (DIP-73xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.385.539	Management appliance 2U without HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.385.540	Management appliance 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-7388-8HD	F.01U.385.541	Management appliance 2U 8X8 TB
DIVAR IP all-in-one 7000	DIP-738C-8HD	F.01U.385.542	Management appliance 2U 8X12 TB
DIVAR IP all-in-one 7000	DIP-73G0-00N	F.01U.385.543	Management appliance 3U without HD
DIVAR IP all-in-one 7000	DIP-73G8-16HD	F.01U.385.544	Management appliance 3U 16X8TB
DIVAR IP all-in-one 7000	DIP-73GC-16HD	F.01U.385.545	Management appliance 3U 16X12 TB

DIVAR IP all-in-one 7000 (DIP-74xx)

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-74C0-00N	F.01U.417.248	Management appliance, 2U w/o HDD
DIVAR IP all-in-one 7000	DIP-74C4-8HD	F.01U.417.249	Management appliance, 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-74C8-8HD	F.01U.417.250	Management appliance, 2U 8X8TB
DIVAR IP all-in-one 7000	DIP-74CI-8HD	F.01U.417.251	Management appliance, 2U 8X18TB
DIVAR IP all-in-one 7000	DIP-74CI-12HD	F.01U.417.252	Management appliance, 2U 12X18TB
DIVAR IP all-in-one 7000	DIP-74G0-00N	F.01U.417.253	Management appliance, 3U w/o HDD
DIVAR IP all-in-one 7000	DIP-74GI-16HD	F.01U.417.254	Management appliance, 3U 16X18TB

Document Change Log

2024.09.04 – Revision 1.00: Initial Release