



CVE-2013-4866

Published on: 04/16/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

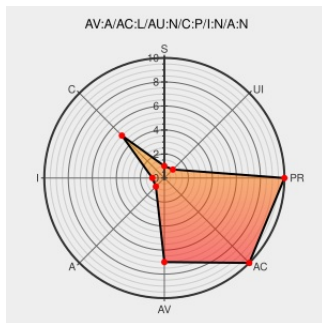
CVE-2013-4866

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [My Satis Genius Toilet](#) from [Lixil](#) contain the following vulnerability:

The LIXIL Corporation My SATIS Genius Toilet application for Android has a hardcoded Bluetooth PIN, which allows physically proximate attackers to trigger physical resource consumption (water or heat) or user discomfort.

CVE-2013-4866 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Full Disclosure: TWSL2013-020: Hard-Coded Bluetooth PIN Vulnerability in LIXIL Satis Toilet

[seclists.org](#)
[text/html](#)

[FULLDISC 20130801 TWSL2013-020: Hard-Coded Bluetooth PIN Vulnerability in LIXIL Satis Toilet](#)

Now even toilets aren't safe from hacking - Features - Gadgets & Tech - The Independent

[www.independent.co.uk](#)
[text/html](#)

[MISC www.independent.co.uk/life-style/gadgets-and-tech/features/now-even-toilets-arent-safe-from-hacking-8747232.html](#)

'Genius Toilet' Can Be Hacked, Can Attack You On The Loo (VIDEO)

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[MISC www.huffingtonpost.co.uk/2013/08/05/smart-toilet-could-attackmy-satis_n_3706116.html](#)

Holy sh*t! Smart toilet hack attack! | Ars Technica

[arstechnica.com](#)
[text/html](#)

[MISC arstechnica.com/security/2013/08/holy-sht-smart-toilet-hack-attack/](#)

404 Not Found | Trustwave

[www.trustwave.com](#)
[text/plain](#)
Inactive Link **Not Archived**

[MISC www.trustwave.com/spiderlabs/advisories/TWSL2013-020.txt](#)

LIXIL Satis Toilet Hard-Coded Bluetooth PIN ≈
Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com/text/html)
text/html

 [MISC packetstormsecurity.com/files/122655/LIXIL-Satis-Toilet-Hard-Coded-Bluetooth-PIN.html](https://packetstormsecurity.com/files/122655/LIXIL-Satis-Toilet-Hard-Coded-Bluetooth-PIN.html)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lixil	My Satis Genius Toilet	-	All	All	All
Application	Lixil	My Satis Genius Toilet	-	All	All	All

cpe:2.3:a:lixil:my_satis_genius_toilet:-:*:*:*:android:*:*:

cpe:2.3:a:lixil:my_satis_genius_toilet:-:*:*:*:android:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)